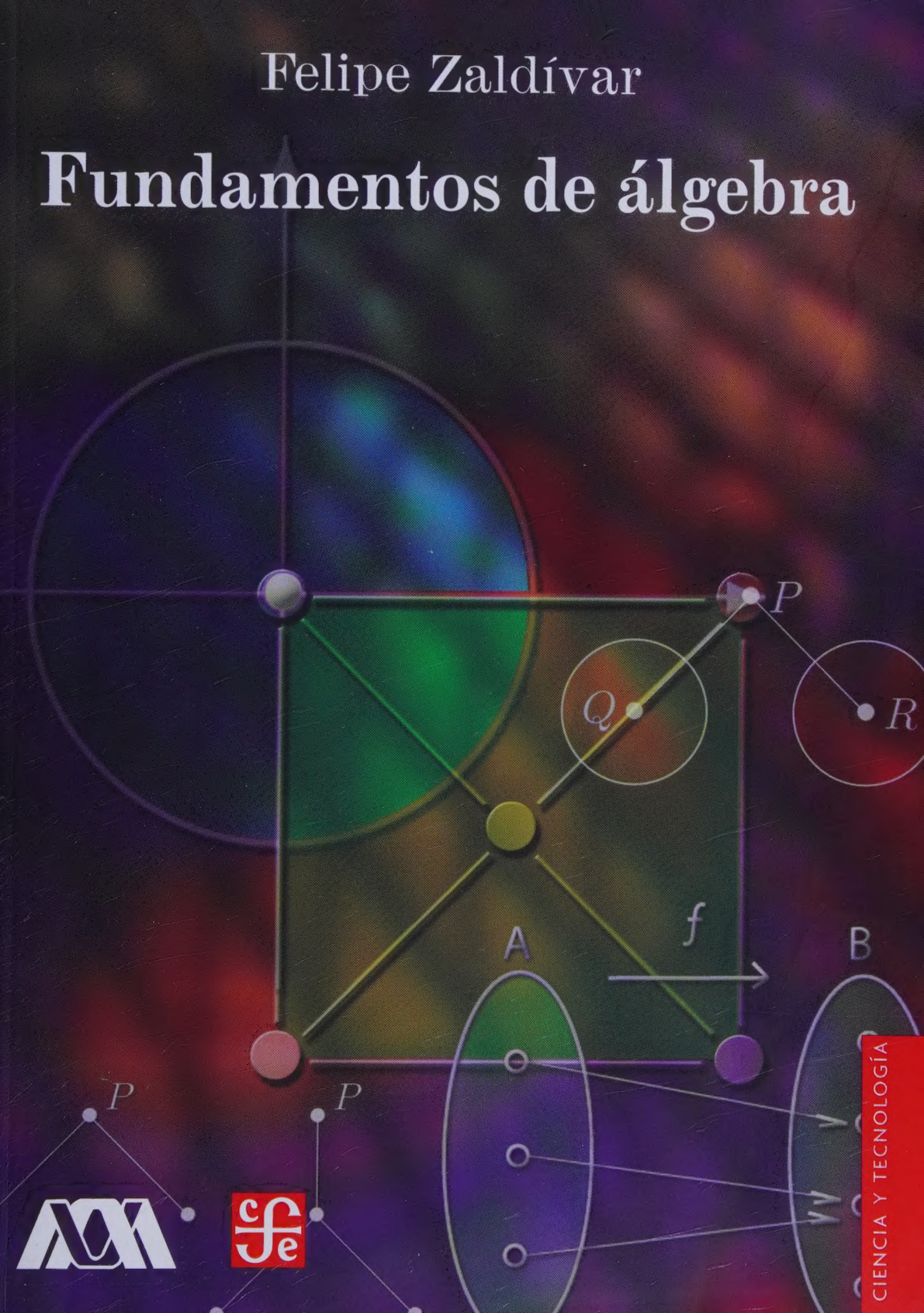
Felipe Zaldívar

Fundamentos de álgebra



CIENCIA Y TECNOLOGÍA

Digitized by the Internet Archive
in 2024

https://archive.org/details/fundamentosdealg0000feli

Sección de Obras de Ciencia y Tecnología

FUNDAMENTOS DE ÁLGEBRA

Comité de Selección

Dr. Antonio Alonso
Dr. Francisco Bolívar Zapata
Dr. Javier Bracho
Dr. Juan Luis Cifuentes
Dra. Rosalinda Contreras
Dr. Jorge Flores Valdés
Dr. Juan Ramón de la Fuente
Dr. Leopoldo García-Colín Scherer
Dr. Adolfo Guzmán Arenas
Dr. Gonzalo Halffter
Dr. Jaime Martuscelli
Dra. Isaura Meza
Dr. José Luis Morán-López
Dr. Héctor Nava Jaimes
Dr. Manuel Peimbert
Dr. José Antonio de la Peña
Dr. Ruy Pérez Tamayo
Dr. Julio Rubio Oca
Dr. José Sarukhán
Dr. Guillermo Soberón
Dr. Elías Trabulse

Coordinadora

María del Carmen Farías R.

FELIPE ZALDÍVAR

Fundamentos de álgebra

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

FONDO DE CULTURA ECONÓMICA

Primera edición: 2005

Zaldívar, Felipe
Fundamentos de álgebra / Felipe Zaldívar — México : FCE, UAM, 2005
318 p. : ilus. ; 23 × 17 cm — (Colec. Sección de Obras de Ciencia y Tecnología)
ISBN 968-16-7826-5

1. Álgebra 2. Matemáticas 3. Lógica I. Ser. II. t.

LC QA341 Dewey 512 Z324f

Distribución mundial

Diseño de portada: *Guadalupe Villa*

Conozca nuestro catálogo en
`http://www.fondodeculturaeconomica.com`

Agradecemos sus comentarios y sugerencias al correo electrónico
`laciencia@fondodeculturaeconomica.com`

Se prohíbe la reproducción total o parcial de esta obra —incluido el diseño tipográfico y de portada—, sea cual fuere el medio, electrónico o mecánico, sin el consentimiento por escrito del editor.

D.R. ©, 2005, Universidad Autónoma Metropolitana
Prolongación Canal de Miramontes N° 3855
Colonia Ex Hacienda de San Juan de Dios,
Delegación Tlalpan, Código Postal 14387,
México, Distrito Federal

D.R. ©, 2005, Fondo de Cultura Económica
Carretera Picacho-Ajusco 227, 14200 México, D.F.

ISBN 968-16-7826-5

Impreso en México • *Printed in Mexico*

ÍNDICE GENERAL

Prólogo 9

I. Conjuntos, relaciones y funciones 13
I.1 Lógica 13
I.2 Conjuntos 19
I.3 Relaciones de equivalencia 29
I.4 Funciones 38

II. Los números naturales 51
II.1 Operaciones en $\mathbb{N}$ 56
II.2 El orden en $\mathbb{N}$ 62
II.3 Otras formulaciones del axioma de inducción 64
II.4 El principio del buen orden 70
II.5 Contar 74
II.6 Principios elementales de conteo 77
II.6.1 Ordenaciones y permutaciones 89
II.6.2 Combinaciones 93
II.6.3 El principio de inclusión-exclusión 101
II.7 Proyecto 1: Recurrencia y funciones generadoras 108
II.8 Bibliografía 125

III. El anillo de números enteros 127
III.1 Operaciones en $\mathbb{Z}$ 128
III.2 El orden en $\mathbb{Z}$ 136
III.3 Dominios enteros 139
III.4 Divisibilidad en $\mathbb{Z}$ 143
III.5 El teorema fundamental de la aritmética 151
III.6 Ecuaciones diofantinas 158
III.7 Congruencias y aritmética modular 162
III.8 Congruencias lineales 168
III.9 Proyecto 2: Criptografía de clave pública 174
III.10 Bibliografía 195

IV. El campo de números racionales 197
IV.1 Operaciones en $\mathbb{Q}$ 198
IV.2 El orden en $\mathbb{Q}$ 201

V. El campo de números reales 207
V.1 Sucesiones en $\mathbb{Q}$ 208
V.2 El campo de números reales 214
V.3 El orden en $\mathbb{R}$ 217
V.4 Completez de $\mathbb{R}$ 219
V.5 Proyecto 3: Los números p-ádicos 226
V.5.1 Bibliografía 232
V.6 Apéndice: El campo $\mathbb{R}$, un enfoque axiomático 232
V.6.1 Propiedades de campo de $\mathbb{R}$ 232
V.6.2 Campos ordenados 237
V.6.3 Campos ordenados completos 241
V.6.4 Bibliografía 246

VI. El campo de números complejos 247
VI.1 El campo de números complejos 247
VI.2 Forma polar de un número complejo 257

VII. Polinomios 267
VII.1 Divisibilidad en anillos de polinomios 270
VII.2 Raíces o ceros de un polinomio 276
VII.2.1 Derivadas de polinomios y multiplicidad de raíces 281
VII.3 Expansión de Taylor de un polinomio 282
VII.4 Coeficientes y raíces 284
VII.5 Polinomios con coeficientes complejos 287
VII.6 El campo de funciones racionales en una variable 290
VII.7 Proyecto 4: Polinomios truncados y criptosistemas . . . 295
VII.7.1 Bibliografía 307
VII.8 Proyecto 5: Registros de corrimiento 307

Bibliografía 313

Índice de términos 315

PRÓLOGO

Double, double, toil and trouble;
Fire burn, and cauldron bubble.

Macbeth, IV.1

En años recientes se han dado varios cambios en los cursos que se imparten en la licenciatura en matemáticas, en especial se han creado algunos cursos diseñados para introducir al estudiante en algunas de las ideas y métodos del pensar matemático cuando el alumno recién ha ingresado a la universidad. Algunos de estos cursos retoman ideas y contenidos de cursos que tradicionalmente se han impartido en otras universidades adaptándolas a los tiempos y circunstancias en este principio de siglo. Al impartir algunos de estos cursos, la experiencia en el salón de clases y la interacción con los alumnos nos llevó a la idea de escribir un texto donde las ideas matemáticas se trataran, desde el principio, con un hilo conductor visible y donde el estudiante fuera un participante activo.

En este libro se parte de unas ideas sencillas de lógica y conjuntos que formalizan, hasta donde es posible en un nivel elemental, el lenguaje que se usará a todo lo largo y ancho del texto (y más allá), incluyendo la notación e ideas básicas de la teoría de conjuntos que permea la matemática. Una vez desarrollado lo anterior, el libro comienza propiamente: relaciones y funciones son conceptos fundamentales en toda la matemática y se discuten con la amplitud necesaria. Después, usando el lenguaje e ideas anteriores, empieza el estudio de las estructuras numéricas: números naturales, enteros, racionales, reales y complejos. El método es simple: se comienza elementalmente y se avanza construyendo sobre lo discutido previamente; a veces hay repeticiones de ideas o métodos: esto es intencional para que el estudiante descubra las estructuras elementales de la matemática y, después de poco tiempo, ya se puedan ir dejando varios detalles de los desarrollos al estudiante. Hay una línea bien marcada que va desde los números naturales hasta los números complejos, sin omitir detalles en el camino (por ejemplo, los números reales se construyen con ideas sencillas adaptadas al nivel del libro).

A lo largo del texto se incluyen ejercicios que complementan lo discutido previamente. Los ejercicios son importantes y se requiere que los estudiantes los vayan haciendo conforme avanza el libro: la matemática es un deporte de participantes y no de espectadores. También se han incluido algunos temas, bajo el nombre de *proyectos*, con la idea de que pueden ser omitidos en una primera lectura, y de hecho se sugieren como lecturas adicionales para el estudiante, fuera de clases, individualmente o en equipo; algunos de estos proyectos exigen más del estudiante y las ideas involucradas sólo se han bosquejado y los ejercicios demandan más involucramiento y madurez, de tal forma que a veces habrá que esperar algún tiempo para su comprensión cabal, por el momento dejando ideas abiertas que motivarán desarrollos posteriores para lo cual hemos incluido algunas referencias bibliográficas que complementan y amplían los temas discutidos en estos proyectos. Regresando al texto propio, notamos que algunos ejercicios duplican ideas ya discutidas, otros las complementan y otros más introducen ideas nuevas que se desarrollarán en cursos posteriores. Por ejemplo, en el capítulo II, la idea de *contar* motiva la existencia de los números naturales y ciertas ideas combinatorias lo ilustran; sin embargo, aquí sólo se encontrarán unos pocos párrafos y ejercicios de matemática combinatoria. Tiempo habrá para que el estudiante profundice esto después. Otro ejemplo es el concepto de *grupo* que de alguna forma está presente desde el capítulo I y, sin embargo, no se le ha definido en forma explícita, aun cuando hay temas que bien lo hubieran requerido. De nuevo, el tiempo llegará cuando este importante concepto aparezca y quizás el joven lector de este libro mirará hacia atrás y leerá las líneas donde el concepto estaba presente-ausente. Si así sucediera, alguna de las metas del libro se habrá alcanzado.

Agradecimientos. De las muchas cosas que le debo a Helen y Dan —además de su curiosidad por algunos temas de este libro—, los dibujos incluidos son de Dan, la cita de Shakespeare es de Helen (que cuando debía estudiar álgebra prefería leer a Camus, lo cual yo siempre aprobaría), y varias conversaciones animadas sobre nuestras lecturas de Tolkien, en diferentes épocas, incluyendo los versos

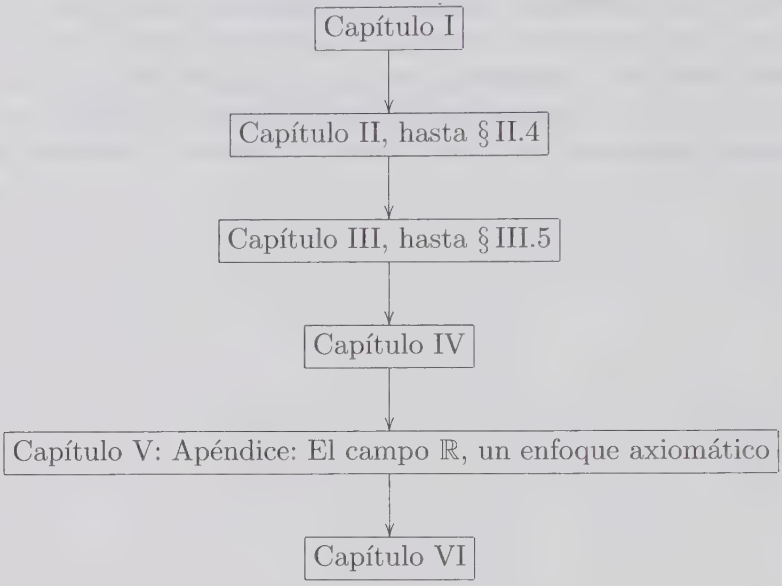
One ring to rule them all, One ring to find them,
One ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

cada vez que yo hablaba de *anillos*.

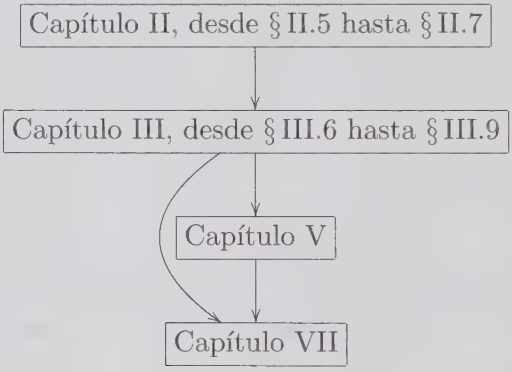
Mis colegas M. J. Arroyo, A. García, L. Hidalgo, G. Izquierdo, B. Llano, H. Martínez, M. Pineda, A. Reyes, J. Solís y A. Wawrzyńczyk usaron versiones preliminares del texto en sus cursos y sus observaciones, comentarios y sugerencias han contribuido a mejorar la presentación y disminuir el número de errores tipográficos, para beneficio del lector y del autor.

Quiero agradecer especialmente el apoyo profesional de la Lic. María del Carmen Farías, responsable del Área de Ciencias del FCE, y a Axel Retif por su paciencia y comprensión en la formación y edición en TEX del manuscrito final.

Sugerencias. Este libro se puede usar en varios cursos, cambiando el orden de la lectura de sus capítulos y secciones. Un primer curso puede estructurarse como sigue:



Un segundo curso se puede estructurar con las secciones faltantes:



I. CONJUNTOS, RELACIONES Y FUNCIONES

En este capítulo se introducen algunos conceptos y métodos que se usarán a lo largo de todo el libro, comenzando con algunos resultados elementales de lógica que nos serán útiles en el análisis y construcción de argumentos; estos resultados serán usados inmediatamente en la introducción del lenguaje y notación de conjuntos. Una vez establecido lo anterior, se introduce el importante concepto de relación entre conjuntos, en particular se estudian las relaciones de equivalencia y las funciones, conceptos de fundamental importancia en toda la matemática.

I.1 Lógica

Esta sección es un resumen de algunos resultados elementales de lógica necesarios para el estudio que emprenderemos. En las líneas siguientes no hay la intención de estudiar propiamente la lógica matemática: sólo se recuerdan o introducen algunos conceptos e ideas que aclaran el uso común de ciertos términos lógicos. La lógica podemos pensarla como el estudio y análisis de los métodos de razonamiento: en todo el libro encontraremos argumentos para probar ciertos resultados y la lógica nos provee de métodos para analizar la corrección de estos argumentos. En forma simplificada pensaremos que un argumento es un conjunto de afirmaciones encadenadas de tal forma que partiendo de ciertas hipótesis, llamadas premisas, al final se obtiene una cierta afirmación (llamada conclusión) y la lógica garantiza que la estructura por medio de la cual se enlazan las afirmaciones de este argumento sea correcta, de tal forma que la conclusión sea en efecto consecuencia de las premisas. A la lógica propiamente no le interesa si las premisas o la conclusión son verdaderas o falsas: lo único que interesa es la validez del argumento.

La (pequeña) parte de la lógica que usaremos se refiere a ciertas afirmaciones sobre objetos dados y requerimos que estas afirmaciones sean de tal forma que podamos decir si son *verdaderas o falsas*. A estas afirmaciones las

llamamos *proposiciones*. Las afirmaciones siguientes son ejemplos de proposiciones:

(1) *El número 6 es par.*

(2) *El número 8 es primo.*

Algunas oraciones o afirmaciones como: *mañana tal vez estudie* no se puede decir si son falsas o verdaderas y así no las consideraremos proposiciones.

Usaremos letras como p, q, r para denotar a las proposiciones y tablas como la que sigue para denotar los *valores verdadero* v o *falso* f que puede tomar una proposición:

p
v
f

Las proposiciones pueden combinarse entre sí para dar lugar a nuevas proposiciones. Las operaciones con proposiciones que nosotros consideraremos son las siguientes:

Negación. Dada una proposición p, su *negación*, denotada $\neg p$ (se lee: no-p) es la proposición que tiene los valores de verdad opuestos a los de p. La tabla siguiente denota lo anterior:

p	$\neg p$
v	f
f	v

Ejemplo 1.

p: 7 es un número primo.

$\neg p$: 7 *no* es un número primo.

Conjunción. Dadas dos proposiciones p, q, su *conjunción* denotada $p \wedge q$ (se lee: p y q) es la proposición que es v sólo cuando ambas proposiciones p, q son verdaderas, y es f cuando alguna de ellas es falsa. Su tabla de verdad es:

p	q	$p \wedge q$
v	v	v
v	f	f
f	v	f
f	f	f

Disyunción. Dadas dos proposiciones p, q, su *disyunción* denotada $p \vee q$ (se lee: p o q) es la proposición que es v cuando alguna de las proposiciones p, q es verdadera y es f únicamente cuando las dos son falsas. Su tabla de verdad es:

p	q	$p \vee q$
v	v	v
v	f	v
f	v	v
f	f	f

Implicación. Dadas dos proposiciones p, q, la *implicación* denotada $p \Rightarrow q$ (se lee: p implica q o si p entonces q o q se sigue de p) es la proposición que es f cuando la hipótesis p es v y la conclusión q es f y es v en todos los otros casos, en particular es v en todos los casos cuando la hipótesis es f. Su tabla de verdad es:

p	q	$p \Rightarrow q$
v	v	v
v	f	f
f	v	v
f	f	v

Equivalencia. Dadas dos proposiciones p, q, diremos que son *equivalentes*, denotado $p \Leftrightarrow q$ (se lee: p equivalente a q o p si y sólo si q) cuando ambas proposiciones p y q tengan los mismos valores de verdad. Su tabla de verdad es:

p	q	$p \Leftrightarrow q$
v	v	v
v	f	f
f	v	f
f	f	v

Observaciones. Las definiciones anteriores se deben tomar como definiciones del uso lógico de las palabras: *no, y, o, implica, equivalente.* Se suelen llamar *conectivos lógicos* a estas palabras.

Notemos ahora que al tomar dos proposiciones sus valores de verdad se combinan en cuatro posibilidades. En general, dadas n proposiciones aceptaremos que sus valores de verdad se combinan en 2^n posibilidades y las distribuiremos comenzando con la mitad de v y luego la mitad de f para la primera proposición, después la cuarta parte de v y de f alternando para la segunda proposición, etcétera.

Al combinar más de dos proposiciones usaremos paréntesis para indicar claramente cómo son las combinaciones para cada par individual y en el orden que se quieren hacer las operaciones. Veamos unos ejemplos:

Ejemplo 2. Escribir la tabla de verdad de la proposición $(p \wedge q) \vee r$. Para esto, notamos que aquí tenemos $n = 3$ proposiciones por lo que hay $2^3 = 8$ combinaciones de sus valores de verdad, las cuales listamos en las primeras tres columnas de la tabla siguiente. La cuarta columna la obtenemos de la definición de la conjunción $p \wedge q$, y la última columna la obtenemos de la definición de disyunción usando ahora los valores de verdad de la cuarta columna y de la tercera:

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$
v	v	v	v	v
v	v	f	v	v
v	f	v	f	v
v	f	f	f	f
f	v	v	f	v
f	v	f	f	f
f	f	v	f	v
f	f	f	f	f

Fórmulas usuales. A continuación listamos algunas equivalencias que usaremos constantemente. Por supuesto que para mostrar que en efecto son equivalencias debemos mostrar que sus valores de verdad son los mismos y para esto hay que construir sus tablas de verdad (nótese que aquí hemos denotado a la equivalencia $\Leftrightarrow$ como $=$; a veces usamos esta notación alterna). Esto lo dejamos como ejercicios para la lectora o lector:

EJERCICIO 1. Usando tablas de verdad, compruebe las equivalencias siguientes:

1. $\neg(\neg p) \equiv p$.
2. $p \wedge q \equiv q \wedge p$.
3. $p \vee q \equiv q \vee p$.
4. $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.
5. $(p \Rightarrow q) \equiv (\neg p \vee q)$.
6. $(p \Leftrightarrow q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$.
7. $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$.
8. $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$.
9. $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.
10. $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
11. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.
12. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.

A las fórmulas (2) y (3) las llamamos *leyes de conmutatividad* para los conectivos $\wedge$ y $\vee$. A las leyes (7) y (8) las llamamos *leyes de De Morgan*; a las leyes (9) y (10) las llamamos *leyes de asociatividad* para los conectivos $\wedge$ y $\vee$, y a las leyes (11) y (12) las llamamos *leyes de distributividad* para los conectivos involucrados.

Cuantificadores lógicos. Algunos argumentos no se pueden analizar con el cálculo proposicional que hemos visto hasta ahora, un ejemplo clásico es el siguiente:

p: *Todos los hombres son mortales.*
q: *Sócrates es hombre.*
r: *Sócrates es mortal.*

De alguna manera la proposición r se sigue de p y q, pero esto no se puede deducir formalmente del cálculo proposicional visto hasta ahora. El punto importante es que para asignarle valores de verdad a las proposiciones p, q, r sus combinaciones involucran términos nuevos, en este caso el término *todos*, que es parte importante de la estructura interna de la proposición p. Se hace necesario entonces refinar el cálculo proposicional anterior para incluir en el lenguaje formal proposiciones que afirmen algo acerca de *todos* o *algunos* miembros de una cierta clase de objetos. Llamaremos *cuantificadores lógicos* a estas palabras y tenemos dos de ellos:

Cuantificador universal. Si todos los miembros de una clase satisfacen una cierta propiedad, lo denotaremos mediante:

$$\forall x\,(P(x))$$

donde aquí el símbolo $\forall$ se lee *para todo* o *todo*, la letra x es una *variable* que denota no a un miembro particular de una clase, sino a un elemento genérico o arbitrario de la clase en consideración. El símbolo $P(x)$ denota una *propiedad* que debe satisfacer el término x. El valor de verdad de una afirmación de la forma $\forall x\,(P(x))$ es v cuando $P(x)$ sea v para todos los valores posibles de x, y es f cuando $P(x)$ sea f para algún valor de x.

Ejemplo 3. Denotemos con
$H(x)$: *x es un hombre.*
$M(x)$: *x es mortal.*

Entonces, la afirmación: *todos los hombres son mortales* se denota:

$$\forall x\,(H(x) \Rightarrow M(x)).$$

EJERCICIO 2. ¿Cómo se lee la afirmación: $\forall x\,(H(x) \Rightarrow \neg M(x))$?

Cuantificador existencial. Si al menos un elemento x de una cierta clase satisface la propiedad $P(x)$, lo denotamos por:

$$\exists x\,(P(x))$$

donde aquí el símbolo $\exists$ se lee *existe*, el símbolo x es una variable y $P(x)$ es una propiedad sobre el elemento x. De esta forma, el valor de verdad de una afirmación de la forma $\exists x\,(P(x))$ es v cuando $P(x)$ sea v para algún valor de x y es f cuando $P(x)$ sea f para todos los valores de x.

Nótese que las definiciones anteriores nos permiten negar afirmaciones con cuantificadores:

(I) La negación de una afirmación de la forma $\forall x(P(x))$ es:

$$\neg(\forall x\,P(x)) \equiv \exists x\,(\neg P(x)).$$

(II) La negación de una afirmación de la forma $\exists x(P(x))$ es:

$$\neg(\exists x\,P(x)) \equiv \forall x\,(\neg P(x)).$$

Ejemplo 4. Denotemos con

$P(x)$: *x es un entero par* y con $T(x)$: *x es un primo.*

Entonces, la afirmación: *hay primos que son pares* formalmente se denota por:

$$\exists x\,(T(x) \Rightarrow P(x)).$$

EJERCICIO 3. ¿Cómo se lee la afirmación: $\exists x\,(T(x) \Rightarrow \neg P(x))$?

I.2 CONJUNTOS

Esta sección es un resumen de notación y propiedades básicas de la teoría de conjuntos necesarios para los capítulos siguientes. El lenguaje y notación de conjuntos provee un marco natural en el cual se pueden formular las teorías matemáticas que iremos encontrando. Los elementos del lenguaje de la teoría de conjuntos que introduciremos ilustran el uso del lenguaje formal de la lógica que vimos en la sección anterior.

El término *conjunto* lo consideraremos un concepto primitivo no definido (podemos pensarlo como un *agregado* o *familia* de objetos, etc.; sin embargo, los términos *agregado*, *familia*, etc., son de alguna forma sinónimos del término *conjunto*); al pensar en un conjunto, pensaremos en los *miembros* o *elementos* que lo constituyen, de tal forma que desde el inicio hay una relación entre los *elementos* y los *conjuntos*, a saber, un elemento puede *pertenecer* o *no pertenecer* a un conjunto dado. Si denotamos a los conjuntos con letras mayúsculas $A, B, C, \ldots$ y a los elementos con letras minúsculas $a, b, c, \ldots$, la *relación de pertenencia* anterior la denotaremos con el símbolo $\in$. Por ejemplo, si V denota al conjunto de *vocales* del idioma español, entonces la letra e pertenece al conjunto de vocales y esto lo denotamos mediante

$$e \in V.$$

Como la letra b no es vocal, entonces no pertenece al conjunto de vocales y esto lo denotamos mediante $b \notin V$. En términos lógicos se tiene la negación de la relación de pertenencia:

$$b \notin V \Leftrightarrow \neg(b \in V).$$

Al describir un conjunto podemos *listar* sus elementos poniéndolos entre llaves, por ejemplo

$$V = \{a, e, i, o, u\}$$

o podemos *describir* el conjunto mediante una *propiedad* que satisfacen únicamente los elementos del conjunto. En este caso se usa la notación:

$$V = \{x \ : \ x \text{ es una vocal}\}.$$

En esta notación, a la que leemos: *V es el conjunto de aquellos elementos x tales que x es una vocal*, observamos lo siguiente:

- x es un elemento genérico (aquí no es la letra x).
- Los dos puntos ":" se leen como *tal que* o *tales que*.
- La propiedad $P(x)$ que satisface x es la que describe genéricamente al conjunto.
- De nuevo usamos llaves para denotar al conjunto en consideración.

Ejemplo 5. El conjunto de enteros positivos lo podemos escribir como:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

donde los puntos suspensivos indican que la lista continúa indefinidamente en la forma indicada. También podemos escribir este conjunto mediante:

$$\mathbb{N} = \{x \ : \ x \text{ es un entero positivo}\}.$$

Ejemplo 6. El conjunto de los enteros primos positivos lo podemos escribir como:

$$B = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$$

listando suficientes elementos para saber de cuáles números se está hablando.

Ejemplo 7. El conjunto de las potencias positivas de 2 lo podemos escribir como:

$$C = \{x \ : \ x = 2^n \text{ con } n \text{ un entero positivo}\} = \{2, 4, 8, 16, 32, \ldots\}.$$

Podemos *comparar* dos conjuntos considerando los elementos que contienen:

Inclusión. Dados dos conjuntos A y B, si sucede que todos los elementos de A también son elementos de B, lo denotamos mediante

$$A \subseteq B$$

y decimos que A es *subconjunto* de B o que A está *contenido* en B. En lenguaje lógico la relación de inclusión anterior está definida por:

$$A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B).$$

La negación de esta relación se denota $A \not\subseteq B$, y así

$$A \not\subseteq B \Leftrightarrow \exists x(x \in A \wedge x \notin B),$$

es decir, $A \not\subseteq B$ si y sólo si existe algún elemento de A que no está en B.

Igualdad. Dados dos conjuntos A y B, diremos que son *iguales*, denotado mediante $A = B$, si $A \subseteq B$ y $B \subseteq A$.

Éste es el momento para introducir un conjunto que, a diferencia de los que hemos considerado hasta ahora, *carece de elementos*:

El conjunto vacío. Un *conjunto vacío* es un conjunto que no tiene elementos. Se suele usar la letra danesa $\emptyset$ para denotar a un conjunto vacío y la propiedad lógica que lo define es:

$$\forall x(x \notin \emptyset)$$

o lo que es lo mismo $\neg(\exists x(x \in \emptyset))$.

A continuación probaremos que sólo hay un conjunto vacío, y para esto probaremos primero que, extraño como parezca a primera vista, un conjunto vacío es subconjunto de cualquier otro conjunto:

PROPOSICIÓN I.1. *Si $\emptyset$ es un conjunto vacío y A es cualquier otro conjunto, entonces $\emptyset \subseteq A$.*

Demostración. Supongamos que la afirmación $\emptyset \subseteq A$ es falsa; entonces su negación $\emptyset \not\subseteq A$ es verdadera. Así, $\exists x \in \emptyset$ tal que $x \notin A$. Pero no es posible que $\exists x \in \emptyset$ ya que $\emptyset$ es vacío. Se sigue que la negación $\emptyset \not\subseteq A$ debe ser falsa, por lo que $\emptyset \subseteq A$ es verdadera. □

Una proposición que es consecuencia (casi) inmediata de otra proposición se suele llamar un *corolario*.

COROLARIO I.2. *Sólo hay un conjunto vacío.*

Demostración. Supongamos que $\emptyset_1$ y $\emptyset_2$ son dos conjuntos vacíos. Como $\emptyset_1$ es vacío y $\emptyset_2$ es otro conjunto, entonces, por la propiedad anterior, $\emptyset_1 \subseteq \emptyset_2$. Invirtiendo los papeles de $\emptyset_1$ y $\emptyset_2$ se tiene que $\emptyset_2 \subseteq \emptyset_1$. Se sigue que $\emptyset_1 = \emptyset_2$. □

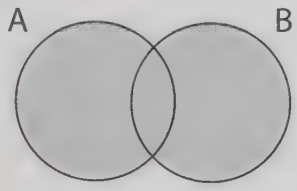
De ahora en adelante podemos hablar *del* conjunto vacío $\emptyset$.

Operaciones con conjuntos. Por medio de las operaciones que describiremos a continuación se obtienen nuevos conjuntos a partir de conjuntos dados.

Unión. Si A, B son conjuntos, la *unión* de A con B es el conjunto

$$A \cup B := \{x \ : \ x \in A \vee x \in B\}.$$

Aquí $\vee$ es la disyunción lógica y así para que un elemento x pertenezca a la unión $A \cup B$ basta con que esté en A o que esté en B. En ocasiones se usan diagramas como el siguiente para denotar a la unión de A con B:



donde el área sombreada denota al nuevo conjunto $A \cup B$.

EJERCICIO 4. Si A, B, C son conjuntos, demuestre que:

(1) $A \cup B = B \cup A$ (conmutatividad de la unión).

(2) $A \cup (B \cup C) = (A \cup B) \cup C$ (asociatividad de la unión).

(3) $A \cup A = A$.

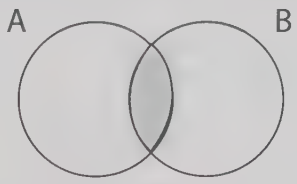
(4) $A \cup \emptyset = A$.

(5) $A \subseteq A \cup B$.

Intersección. Si A, B son conjuntos, la *intersección* de A con B es el conjunto

$$A \cap B := \{x \ : \ x \in A \wedge x \in B\}.$$

Aquí $\wedge$ es la conjunción lógica y así para que un elemento x pertenezca a la intersección $A \cap B$ es necesario que esté en A y que esté en B. En ocasiones se usan diagramas como el siguiente para denotar a la intersección $A \cap B$:



donde el área sombreada indica el conjunto $A \cap B$.

EJERCICIO 5. Si A, B, C son conjuntos, demuestre que:

(1) $A \cap B = B \cap A$ (conmutatividad de la intersección).

(2) $A \cap (B \cap C) = (A \cap B) \cap C$ (asociatividad de la intersección).

(3) $A \cap A = A$.

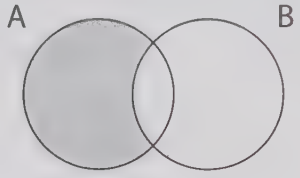
(4) $A \cap \emptyset = \emptyset$.

(5) $A \cap B \subseteq A$.

Diferencia. Si A, B son conjuntos, la *diferencia* de A con B es el conjunto

$$A - B := \{x \ : \ x \in A \wedge x \notin B\}.$$

Aquí $\wedge$ es la conjunción lógica y así para que un elemento x pertenezca a la diferencia $A - B$ se requiere que esté en A y que no esté en B. En ocasiones se usan diagramas como el siguiente para denotar a la diferencia $A - B$:



donde el área sombreada indica el conjunto $A - B$.

EJERCICIO 6. Si A, B son conjuntos, demuestre que:

(1) $A - A = \emptyset$.

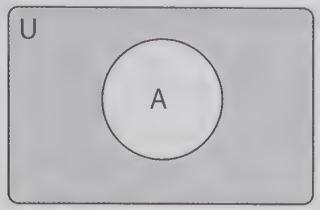
(2) $A - \emptyset = A$.

(3) $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$.

Complemento. Si todos los conjuntos que se están considerando en una cierta situación son subconjuntos de un conjunto dado U y si $A \subseteq U$, el *complemento* de A en U es la diferencia

$$A^c := \{x \ : \ x \in U \wedge x \notin A\} = U - A.$$

En ocasiones se usan diagramas como el siguiente para denotar al complemento A^c:



donde el área sombreada indica el conjunto A^c.

EJERCICIO 7. Si $A \subseteq U$, demuestre que:

(1) $(A^c)^c = A$.

(2) $\emptyset^c = U$.

(3) $U^c = \emptyset$.

(4) $A \cup A^c = U$.

(5) $A \cap A^c = \emptyset$.

(6) Si $B \subseteq U$ es otro conjunto, $A - B = A \cap B^c$.

A continuación probamos algunas propiedades importantes de estas operaciones:

PROPOSICIÓN I.3. *Si A, B, C son subconjuntos de un conjunto U, entonces:*

(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(3) $(A \cap B)^c = A^c \cup B^c$.

(4) $(A \cup B)^c = A^c \cap B^c$.

Las propiedades (1) y (2) se llaman las *leyes distributivas* para la intersección y la unión de conjuntos. Las propiedades (3) y (4) son las *leyes de De Morgan.*

Demostración. Probaremos (1) y (3). Para (1), mostraremos primero que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. En efecto, dado cualquier $x \in A \cap (B \cup C)$ entonces por definición de intersección $x \in A \wedge x \in (B \cup C)$ y por definición de unión

$$x \in A \wedge (x \in B \vee x \in C)$$

y usando la ley distributiva de los conectivos lógicos $\wedge$ y $\vee$ se sigue que

$$(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$$

es decir,

$$(x \in (A \cap B)) \vee (x \in (A \cap C))$$

i.e., $x \in ((A \cap B) \cup (A \cap C))$, y por lo tanto $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Para la otra inclusión $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ se procede en forma similar.

Para (3), mostraremos primero que $(A \cap B)^c \subseteq A^c \cup B^c$. En efecto, si $x \in (A \cap B)^c$ por definición de complemento $x \notin (A \cap B)$ y usando los conectivos lógicos que definen la intersección y la negación se tiene que: $x \notin A \vee x \notin B$, por lo que $x \in A^c$ o $x \in B^c$ por definición de complemento; se sigue, por definición de unión, que $x \in A^c \cup B^c$ y por lo tanto $(A \cap B)^c \subseteq A^c \cup B^c$.

Para la otra inclusión $A^c \cup B^c \subseteq (A \cap B)^c$ se procede en forma similar. □

EJERCICIO 8. Demuestre las otras dos propiedades faltantes en la proposición anterior.

Familias de conjuntos. En ocasiones se tienen varios conjuntos y conviene, por ejemplo si se tienen diez conjuntos, denotarlos con subíndices: A_1, A_2,..., A_{10} y se puede obtener su unión y su intersección, usando las propiedades de asociatividad, mediante:

$$A_1 \cup A_2 \cup \cdots \cup A_{10}$$

y

$$A_1 \cap A_2 \cap \cdots \cap A_{10}.$$

En general, si se tienen n conjuntos podemos abreviar lo anterior escribiendo:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

y

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

observando que la notación de la parte izquierda es más económica, de tal manera que esta notación es la que usaremos cuando se tiene una familia infinita de conjuntos, por ejemplo si se tienen conjuntos $A_1, A_2, \ldots, A_i, \ldots$, donde los índices son elementos del conjunto de los enteros positivos $\mathbb{N}$, las operaciones anteriores se denotan:

$$\bigcup_{i\in\mathbb{N}} A_i \qquad \text{y} \qquad \bigcap_{i\in\mathbb{N}} A_i.$$

En general se puede tener un conjunto de índices arbitrario, digamos I, y para cada índice $\alpha \in I$ se tiene un conjunto A_α. En esta situación diremos que los conjuntos A_α con $\alpha \in I$ forman una *familia de conjuntos indicada por el conjunto de índices* I. En los tres ejemplos previos el conjunto de índices es $I = \{1, 2, 3, \ldots, 10\}$, $I = \{1, 2, 3, \ldots, n\}$ e $I = \mathbb{N}$.

La unión de una familia de conjuntos A_α, $\alpha \in I$, es el conjunto:

$$\bigcup_{\alpha\in I} A_\alpha := \{x \ : \ \exists \alpha \in I \text{ con } x \in A_\alpha\},$$

es decir, x pertenece a la unión de la familia si y sólo si x está en algún A_α:

$$x \in \bigcup_{\alpha\in I} A_\alpha \Leftrightarrow \exists \alpha \in I \ \text{ tal que } \ x \in A_\alpha.$$

La intersección de la familia es el conjunto:

$$\bigcap_{\alpha\in I} A_\alpha := \{x \ : \ \forall \alpha \in I \text{ se tiene que } x \in A_\alpha\},$$

es decir, x pertenece a la intersección de la familia si y sólo si x está en todos los conjuntos de la familia A_α:

$$x \in \bigcap_{\alpha\in I} A_\alpha \Leftrightarrow \forall \alpha \in I \ \text{ se tiene que } \ x \in A_\alpha.$$

Recordando las negaciones de los cuantificadores lógicos y las definiciones anteriores se tiene que:

$$x \notin \bigcup_{\alpha\in I} A_\alpha \Leftrightarrow \forall \alpha \in I \ \text{ se tiene que } \ x \notin A_\alpha$$

y

$$x \notin \bigcap_{\alpha\in I} A_\alpha \Leftrightarrow \exists \alpha \in I \ \text{ tal que } \ x \notin A_\alpha.$$

EJERCICIO 9. Si A_α, $\alpha \in I$ es una familia de conjuntos y M es cualquier otro conjunto, demuestre que:

(1) $M \cap \left(\bigcup_{\alpha\in I} A_\alpha\right) = \bigcup_{\alpha\in I}(M \cap A_\alpha)$. .

(2) $M \cup \left(\bigcap_{\alpha\in I} A_\alpha\right) = \bigcap_{\alpha\in I}(M \cup A_\alpha)$.

Si A_α, $\alpha \in I$ es una familia de conjuntos todos contenidos en un conjunto U, demuestre que:

(3) $\left(\bigcup_{\alpha\in I} A_\alpha\right)^c = \bigcap_{\alpha\in I} A_\alpha^c$.

(4) $\left(\bigcap_{\alpha\in I} A_\alpha\right)^c = \bigcup_{\alpha\in I} A_\alpha^c$.

EJERCICIO 10. Si A, B son conjuntos, se define la *diferencia simétrica* entre A y B mediante

$$A \triangle B := (A - B) \cup (B - A).$$

Demuestre que:

(I) La operación $\triangle$ es asociativa, es decir,

$$A \triangle (B \triangle C) = (A \triangle B) \triangle C,$$

para cualesquiera conjuntos A, B, C.

(II) La operación $\triangle$ es conmutativa, es decir,

$$A \triangle B = B \triangle A,$$

para cualesquiera conjuntos A, B.

(III) $A \triangle \emptyset = A$, para cualquier conjunto A.

(IV) $A \triangle A = \emptyset$, para cualquier conjunto A.

I.3 Relaciones de equivalencia

Dados dos conjuntos A y B para formalizar la noción de *relación* entre elementos de A con elementos de B necesitaremos la noción de par ordenado. Para esto observemos que si $a \in A$ y $b \in B$, se tiene que $\{a, b\} = \{b, a\}$, y si $a \neq b$, diremos que el conjunto $\{a, b\}$ es un par no ordenado. También notamos que si sucediera que $a = b$, entonces $\{a, a\} = \{a\}$ y ni siquiera podemos hablar en este caso de un par no ordenado. El concepto de *par ordenado* se introduce para distinguir los elementos del conjunto $\{a, b\}$ de tal forma que se tenga un primer elemento y un segundo elemento. Se suele usar la notación

$$(a, b)$$

para denotar al par ordenado cuya *primera componente* es a y cuya *segunda componente* es b. La propiedad definitoria de este par ordenado nos dice que *dos pares ordenados (a, b) y (c, d) son iguales si y sólo si componente a componente son iguales.* En símbolos:

$$(*) \qquad (a, b) = (c, d) \Leftrightarrow a = c \ \wedge \ b = d.$$

Siendo más formales, adoptaremos la definición de K. Kuratowski de un par ordenado en términos de la notación y lenguaje desarrollados hasta ahora. Dados elementos $a \in A, b \in B$ se define

$$(a, b) := \{\{a\}, \{a, b\}\},$$

es decir, (a, b) es el conjunto cuyos elementos son los conjuntos $\{a\}$ y $\{a, b\}$. Esta definición sólo usa la notación y lenguaje introducidos previamente y notamos que satisface la condición definitoria $(*)$:

Proposición I.4. $(a, b) = (c, d) \Leftrightarrow a = c \ \wedge \ b = d.$

Demostración. La implicación $(\Leftarrow)$ es obvia. Para la otra implicación, si $(a, b) = (c, d)$ entonces $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ y así se tienen dos casos:

(1) $\{a\} = \{c\}$ y $\{a, b\} = \{c, d\}$; se tiene entonces que $a = c$ por lo que $\{a, b\} = \{a, d\}$ y así $b = d$.

(2) $\{a\} = \{c, d\}$ y $\{a, b\} = \{c\}$; se tiene entonces que $a = c = d = b$. □

Producto cartesiano. Dados dos conjuntos A, B, se define el *producto cartesiano* de A con B como el conjunto de todos los pares ordenados cuya primera componente está en A y cuya segunda componente está en B; en símbolos:

$$A \times B := \{(a, b) \ : \ a \in A \wedge b \in B\}.$$

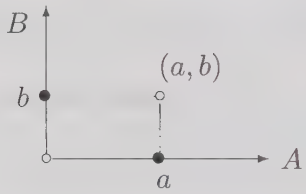
Aquí $A \times B$ se lee: *A cruz B* o *el producto cartesiano* de A con B.

Ejemplo 8. Si $A = \{1, 2\}$ y $B = \{a, b, c\}$, entonces

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$

Nótese que, en general, $A \times B \neq B \times A$: en el ejemplo anterior $(1, a) \in A \times B$ pero $(1, a) \notin B \times A$.

En ocasiones conviene representar geométricamente el producto cartesiano $A \times B$ poniendo en un eje horizontal al conjunto A de primeras componentes y en un eje vertical al conjunto B de las segundas componentes:



En esta representación el par ordenado (a, b) corresponde al punto de abscisa a y ordenada b en el *plano* $A \times B$.

Relaciones. Podemos ahora formalizar el concepto de relación. Dados dos conjuntos A, B, una *relación entre elementos de A y elementos de B* es un subconjunto R del producto cartesiano $A \times B$, *i.e.*, $R \subseteq A \times B$ y así R consiste de algunos pares ordenados (a, b) con $a \in A$ y $b \in B$. Si $(a, b) \in R$ a veces lo denotaremos mediante aRb y decimos que *el elemento a está relacionado con b*. Si $(x, y) \notin R$ lo denotamos $x \not R y$. El *dominio* de una relación R es el conjunto formado por las primeras componentes de los pares ordenados de R. Usaremos la notación D_R para el dominio de R. Así,

$$D_R := \{a \in A \ : \ \text{existe } b \in B \text{ tal que } (a, b) \in R\}.$$

Ejemplo 9. Si A es el conjunto de seres humanos y B es el conjunto de países del mundo, definimos la relación R en $A \times B$ mediante pRq si p es ciudadano de q.

Ejemplo 10. Si A es el conjunto de habitantes de la ciudad de México y B es el conjunto de universidades de la ciudad de México, definimos la relación pRq si p es estudiante en q.

Ejemplo 11. Si $A = B = \mathbb{N}$ es el conjunto de enteros positivos, definimos la relación aRb si a es el doble de b. Por ejemplo, $4R2$, $10R5$, pero $(3,7) \notin \mathrm{R}$. El dominio de esta relación es: $D_R =$ conjunto de enteros positivos pares.

Ejemplo 12. Si $A = B = \mathbb{N}$, definimos la relación aRb si $a < b$ (*i.e.*, si a es menor que b). Por ejemplo $(3,7) \in R$, $(5,6) \in R$ pero $(3,3) \notin R$ y $(7,3) \notin R$. El dominio de esta relación es todo $A = \mathbb{N}$.

Nota. Dados cualesquiera conjuntos A, B, siempre se tienen las relaciones $R = \emptyset$ (la *relación vacía*) y la relación $R = A \times B$ (la *relación total*).

EJERCICIO 11. Si $A = \{1,2\}$ y $B = \{a,b,c\}$, liste todas las relaciones en $A \times B$ y dé sus dominios.

De todas las relaciones entre dos conjuntos hay unas que son muy importantes y consideraremos algunas de éstas. Para comenzar consideraremos sólo relaciones R donde $A = B$ y en este caso diremos que $R \subseteq A \times A$ es *una relación en el conjunto* A.

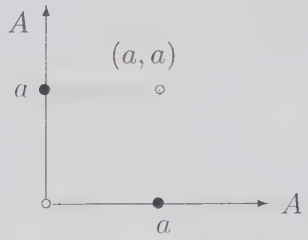
Una relación R en un conjunto A se dice que es:

- *Reflexiva* si para todo $a \in A$ se tiene que aRa.
- *Simétrica* si siempre que aRb se tiene que bRa.
- *Transitiva* si aRb y bRc implican que aRc.
- *Antisimétrica* si aRb y bRa implican que $a = b$.

Ejemplo 13. Si A es cualquier conjunto, se tiene la relación *diagonal* en A dada por

$$\Delta := \{(a, a) \ : \ a \in A\} \subseteq A \times A.$$

Gráficamente, en el "plano" $A \times A$ los pares ordenados de Δ están en la recta diagonal a 45°:



Claramente esta relación es reflexiva, simétrica, transitiva y antisimétrica.

Ejemplo 14. Si $A = \mathbb{N}$, la relación R dada por mRn si m divide a n (denotado: $m|n$) es *reflexiva* ya que para todo $m \in \mathbb{N}$ se tiene que $m|m$. No es simétrica ya que, por ejemplo, $2|8$ pero $8 \nmid 2$ (no divide).

EJERCICIO 12. Muestre que la relación del ejemplo 14 es transitiva y antisimétrica.

EJERCICIO 13. Demuestre que una relación R en un conjunto A es reflexiva si y sólo si contiene a la relación diagonal de A (véase el ejemplo 13).

Ejemplo 15. Denotemos con $\mathbb{Z}$ al conjunto de enteros positivos, negativos y el cero, digamos $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$. En $\mathbb{Z}$ definamos la relación R mediante aRb si $a - b$ es par. Entonces R es reflexiva, simétrica y transitiva.

Relaciones de equivalencia. Una relación R en un conjunto A se dice que es de *equivalencia* si es reflexiva, simétrica y transitiva. Así, la diagonal (ejemplo 13) es una relación de equivalencia en cualquier conjunto A. El ejemplo 15 también es una relación de equivalencia.

Ejemplo 16. En $\mathbb{Z}$ definamos la relación R mediante aRb si $a - b$ es divisible por 5, *i.e.*, si $a - b = 5t$ para algún $t \in \mathbb{Z}$. Esta es una relación de equivalencia ya que:

(I) R es *reflexiva* ya que para todo $a \in \mathbb{Z}$ se tiene que $a - a = 0 = 5(0)$.

(II) R es *simétrica* ya que si aRb entonces $a - b = 5t$ con $t \in \mathbb{Z}$ y así $b - a = (-1)(a - b) = 5(-t)$ con $-t \in \mathbb{Z}$ y así bRa.

(III) R es *transitiva* ya que si aRb y bRc, entonces $a - b = 5t$ y $b - c = 5r$ con $t, r \in \mathbb{Z}$, por lo que sumando estas igualdades obtenemos:

$$a - c = (a - b) + (b - c) = 5t + 5r = 5(t + r) \qquad \text{con } t + r \in \mathbb{Z}$$

y así aRc.

EJERCICIO 14. Fije un entero $m \geq 1$ en $\mathbb{Z}$ y defina la relación siguiente en $\mathbb{Z}$: xRy si m divide a $x - y$, *i.e.*, si $m|x - y$. Demuestre que R es una relación de equivalencia en $\mathbb{Z}$.

EJERCICIO 15. Si A es el conjunto de rectas $\mathcal{L}$ en el plano, la relación $\mathcal{L}_1 \| \mathcal{L}_2$ ($\mathcal{L}_1$ es paralela a $\mathcal{L}_2$) es una relación de equivalencia.

EJERCICIO 16. En $\mathbb{Z}$ defina la relación R mediante aRb si $a \leq b$. Muestre que R es reflexiva, antisimétrica y transitiva.

EJERCICIO 17. Exhiba un ejemplo de una relación R en un conjunto A que sea reflexiva y simétrica pero no transitiva.

EJERCICIO 18. Dé un ejemplo de una relación reflexiva y transitiva pero no simétrica.

¿Existirá un ejemplo de una relación R con dominio A que sea simétrica y transitiva pero no reflexiva?

EJERCICIO 19. En $\mathbb{Z}$ defina la relación aRb si $a + b$ es par. Demuestre que es una relación de equivalencia.

EJERCICIO 20. Si $\mathbb{R}$ denota el conjunto de números reales (quizá ya los estudió en su curso de Cálculo) considere la relación $R \subseteq \mathbb{R} \times \mathbb{R}$ dada por aRb si $a - b \in \mathbb{Z}$ (aquí usamos que $\mathbb{Z} \subseteq \mathbb{R}$). Demuestre que R es una relación de equivalencia.

EJERCICIO 21. En el conjunto $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ defina la relación $R \subseteq \mathbb{R}^2 \times \mathbb{R}^2$ siguiente:

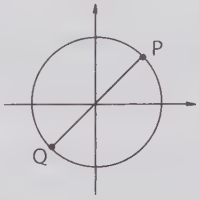
$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a - c \in \mathbb{Z} \text{ y } b - d \in \mathbb{Z}.$$

Demuestre que es una relación de equivalencia.

EJERCICIO 22. Aquí usaremos un poco de geometría. Considere el *círculo unitario* $S^1 \subseteq \mathbb{R}^2$ definido por

$$S^1 := \{(x, y) \in \mathbb{R}^2 \ : \ x^2 + y^2 = 1\}$$

y defina la relación siguiente en S^1: dos puntos $P, Q \in S^1$ están relacionados, denotado $P \sim Q$, si y sólo si P y Q son iguales o están en los extremos opuestos de una diagonal de S^1:



Demuestre que $\sim$ es una relación de equivalencia en S^1.

Clases de equivalencia. Si R es una relación de equivalencia en un conjunto $A \neq \emptyset$, dado un elemento $a \in A$ podemos considerar aquellos elementos de A que estén relacionados con a; denotamos este conjunto con $[a]$ y lo llamamos la *clase de equivalencia de* a:

$$[a] := \{x \in A \ : \ xRa\}.$$

Las clases de equivalencia de R forman una familia de subconjuntos de A que satisface:

(1) Para cada $a \in A$ la clase $[a]$ es no vacía.

(2) Si $[a] \cap [b] \neq \emptyset$, entonces $[a] = [b]$.

(3) $\bigcup_{a \in A} [a] = A$.

Demostración. (1) $a \in [a]$ ya que aRa porque R es reflexiva.

(2) Mostraremos que $[a] \subseteq [b]$. Para esto, sea $x \in [a]$. Así, xRa y como existe un $z \in [a] \cap [b]$ entonces zRa y zRb; por simetría se sigue que aRz y como xRa entonces por transitividad se tiene que xRz, y como zRb, de nuevo por transitividad se sigue que xRb, *i.e.*, $x \in [b]$. Similarmente se prueba que $[b] \subseteq [a]$. Se sigue que $[a] = [b]$.

(3) Como para todo $a \in A$ se tiene que $a \in [a] \subseteq \bigcup_{a\in A}[a]$, entonces $A \subseteq \bigcup_{a\in A}[a]$ y como cada $[a] \subseteq A$, entonces $\bigcup_{a\in A}[a] \subseteq A$. □

A una familia de subconjuntos $A_\alpha \subseteq A$, con $\alpha \in I$ un conjunto de índices, que satisfacen las tres propiedades anteriores:

(1) Cada $A_\alpha \neq \emptyset$.

(2) $A_\alpha \cap A_\beta \neq \emptyset$ implica que $A_\alpha = A_\beta$.

(3) $A = \bigcup_\alpha A_\alpha$,

se le llama una *partición* P del conjunto A.

Arriba mostramos que, dada una relación de equivalencia R en el conjunto A, las clases de equivalencia $[a]$ de esta relación forman una partición del conjunto A a la que llamaremos el *conjunto cociente* de la relación R y lo denotamos por A/R:

$$A/R := \{[a] \ : \ a \in A\}.$$

Hemos así probado la primera parte del teorema siguiente:

TEOREMA I.5. *Sea A un conjunto. Entonces:*

(1) *Toda relación de equivalencia R en A induce una partición A/R en A.*

(2) *Toda partición $P = \{C_\alpha \ : \ C_\alpha \subseteq A\}$ del conjunto A induce una relación de equivalencia en A, a la que denotaremos por R_P.*

Demostración. Sólo falta probar la parte (2). Para esto, pensaremos a cada conjunto de la partición $C_\alpha \subseteq A$ como una (futura) clase de equivalencia de tal forma que es natural entonces definir la relación R_P en A como sigue: dados $a, b \in A$ diremos que aR_Pb si y sólo si existe un C_α tal que $a, b \in C_\alpha$ (*i.e.*, si y sólo si a y b están en el mismo C_α). Claramente R_P es reflexiva y simétrica. Supongamos ahora que aR_Pb y bR_Pc. Entonces $a, b \in C_\alpha$ y $b, c \in C_\beta$. Se sigue que $b \in C_\alpha \cap C_\beta$ por lo que $C_\alpha = C_\beta$ y consecuentemente $a, c \in C_\alpha$, *i.e.*, aR_Pc. □

EJERCICIO 23. Sea A un conjunto y suponga que R y R' son dos relaciones de equivalencia en A que inducen la misma partición. Demuestre que $R = R'$.

EJERCICIO 24. Sea A un conjunto y suponga que P y P' son dos particiones de A que inducen la misma relación de equivalencia. Demuestre que $P = P'$.

Ejemplo 17. Sea $A = \mathbb{Z}$ y consideremos la relación de equivalencia R del ejemplo 16: aRb si $5|a-b$. Queremos determinar su conjunto cociente. Para esto, si $a \in \mathbb{Z}$ su clase de equivalencia es

$$[a] = \{x \in \mathbb{Z} \ : \ xRa\} = \{x \in \mathbb{Z} \ : \ x - a = 5q \ \text{ con } q \in \mathbb{Z}\},$$

en otras palabras, x y a difieren por un múltiplo de 5.

Observemos ahora que al dividir un entero entre 5 sus posibles residuos son $0, 1, 2, 3, 4$. Dado $a \in \mathbb{Z}$ al dividirlo entre 5 digamos que su cociente es q y su residuo es r de tal forma que $a = 5q + r$ con $0 \leq r \leq 4$ y notemos que $5|a - r$ por lo que $[a] = [r]$. Hemos así probado que la clase de equivalencia $[a]$ de un elemento arbitrario $a \in \mathbb{Z}$ es igual a la clase de equivalencia $[r]$ del residuo r que deja a al dividirlo entre 5. Por lo tanto sólo hay cinco posibles clases de equivalencia, a saber $[0], [1], [2], [3], [4]$. Observamos finalmente que estas clases son disjuntas por parejas, ya que si dos de ellas se intersectaran, por ejemplo si $[1] \cap [2] \neq \emptyset$, entonces existiría un $x \in [1] \cap [2]$, *i.e.,* x al dividirlo entre 5 deja residuo 1 y deja residuo 2, lo cual no es posible ya que el residuo debe ser único. Se sigue que $[1] \cap [2] = \emptyset$ y similarmente para los otros pares. Es también fácil ver que $[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$, por lo que el conjunto cociente es:

$$\mathbb{Z}/R = \{[0], [1], [2], [3], [4]\}.$$

EJERCICIO 25. Determine el conjunto cociente de la relación de equivalencia del ejercicio (14).

EJERCICIO 26. Determine el conjunto cociente de la relación de equivalencia del ejercicio (20).

EJERCICIO 27. Determine el conjunto cociente de la relación de equivalencia del ejercicio (21).

EJERCICIO 28. Determine el conjunto cociente de la relación de equivalencia del ejercicio (22).

EJERCICIO 29. Determine si las relaciones R siguientes, definidas en el conjunto A dado, son o no de equivalencia. Si la relación dada es de equivalencia, describa su conjunto cociente:

(I) $A = \mathbb{Z}$, $aRb \Leftrightarrow a \leq b + 1$.

(II) $A = \mathbb{Z}$, $aRb \Leftrightarrow ab > 0$.

(III) $A = \mathbb{Z}$, $aRb \Leftrightarrow ab \geq 0$.

(IV) $A = \mathbb{R}$, $aRb \Leftrightarrow |a| = |b|$ (donde $|\ |$ es el valor absoluto).

(V) $A = \mathbb{R}$, $aRb \Leftrightarrow a^2 + b^2 = 4$.

(VI) $A = \mathbb{Z}$, $aRb \Leftrightarrow a + b$ es impar.

EJERCICIO 30. Si R_1, R_2 son relaciones de equivalencia en un conjunto A, demuestre que $R_1 \cap R_2$ es una relación de equivalencia en A.

EJERCICIO 31. Si R_1, R_2 son relaciones de equivalencia en un conjunto A, ¿es $R_1 \cup R_2$ una relación de equivalencia en A?

EJERCICIO 32. Una relación R en un conjunto A se dice que es *circular* si aRb y bRc implican que cRa. Demuestre que una relación R en A es circular y reflexiva si y sólo si R es de equivalencia.

Relaciones de orden. Una relación $\preceq$ en un conjunto A se dice que es *un orden parcial* si satisface:

(I) Es reflexiva, *i.e.*, $a \preceq a$ para todo $a \in A$.

(II) Es antisimétrica, i.e. $a \preceq b$ y $b \preceq a$ implican que $a = b$.

(III) Es transitiva, *i.e.*, $a \preceq b$ y $b \preceq c$ implican que $a \preceq c$.

Cuando esto suceda, diremos que $(A, \preceq)$ es un *conjunto parcialmente ordenado.*

Ejemplo 18. La relación $\preceq$ en $\mathbb{N}$ dada por $m \preceq n$ si y sólo si $m|n$ es un orden parcial ya que es reflexiva porque $m|m$ para todo $m \in \mathbb{N}$, y si $m|n$ y $n|m$ entonces $m = n$, por lo que la relación es antisimétrica. Finalmente, es transitiva ya que $m|n$ y $n|k$ implican que $m|k$.

Ejemplo 19. Si M es cualquier conjunto y A es la familia de subconjuntos de M, *i.e.*,

$$A = \{R \,:\, R \subseteq M\},$$

dados cualesquiera dos subconjuntos $R, T \in A$, definimos la relación $R \preceq T$ si y sólo si $R \subseteq T$. Éste es un orden parcial en A.

Ejemplo 20. El ejemplo anterior tiene la variación siguiente: dados $R, T \in A$ se define la relación $R \preceq T$ si y sólo si $R \supseteq T$. Éste es otro orden parcial en A.

Ejemplo 21. En el conjunto $\mathbb{N}$ de enteros positivos, definimos la relación $m \leq n$ mediante $m < n$ o $m = n$. Éste es un orden parcial en $\mathbb{N}$.

EJERCICIO 33. En el conjunto $\mathbb{N}$ de enteros positivos, definimos la relación $m \preceq n$ mediante:

$$m \preceq n \Leftrightarrow \begin{cases} m, n \text{ son pares} & \text{y} \quad m \leq n \\ m, n \text{ son impares} & \text{y} \quad m \leq n \\ m \text{ es par} & \text{y} \quad n \text{ es impar.} \end{cases}$$

Muestre que $\preceq$ es un orden parcial en $\mathbb{N}$.

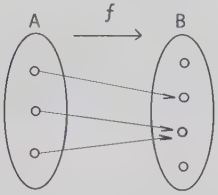
En los capítulos siguientes veremos más acerca de relaciones de orden, en particular en las secciones § II.2 y § II.4.

I.4 FUNCIONES

Una clase muy importante de relaciones entre dos conjuntos es la de las funciones. Si A y B son dos conjuntos, una *función f entre A y B* es una relación $f \subseteq A \times B$ que satisface: para cada $a \in A$ existe un único $b \in B$ tal que $(a, b) \in f$. Nótese en particular que el dominio de f es todo A.

Si f es una función entre A y B lo denotaremos mediante $f : A \to B$. Dado $a \in A$ al único elemento $b \in B$ relacionado, mediante f, con a, lo denotamos $b =: f(a)$ y decimos que b es la *imagen* de a bajo f o que b es el *valor* de f en a. La notación $b = f(a)$ se lee: *b es f de a*. Decimos que $b = f(a)$ es la *regla de correspondencia* de la función f.

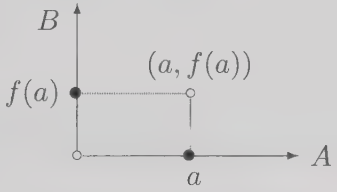
A veces usamos un diagrama como el que sigue para denotar a una función $f : A \to B$



Dada una función $f : A \to B$, el conjunto A es el *dominio* de f y el conjunto B se llama el *codominio* de f. El conjunto de todas las imágenes de f es un subconjunto del codominio B y lo llamamos la *imagen* de f y se denota por $f(A)$; así,

$$f(A) = \{f(a) \ : \ a \in A\} \subseteq B.$$

Como para cualquier relación, podemos representar gráficamente una función en el plano cartesiano $A \times B$, poniendo el dominio en el eje horizontal y el codominio en el eje vertical:



y al conjunto de puntos $\{(a, f(a)) \ : \ a \in A\}$ que, de acuerdo con nuestra definición, es la función f, también lo llamamos la *gráfica* de f.

Ejemplo 22. Si A es cualquier conjunto se tiene la *función identidad* $\mathrm{id}_A : A \to A$ dada por $\mathrm{id}(x) = x$ para $x \in A$.

Ejemplo 23. Si $A = \mathbb{N}$, la relación $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n$ es una función ya que cada número natural tiene un único doble.

Ejemplo 24. La relación $g : \mathbb{Z} \to \mathbb{Z}$ dada por $g(x) = x^2$ es una función ya que cada entero tiene un único cuadrado.

Ejemplo 25. La relación $h : \mathbb{N} \to \mathbb{N}$ dada por la regla $(x, y) \in h$ si y sólo si $x \leq y$, no es una función ya que, por ejemplo, si $x = 4$ se tiene que $(4, 4)$, $(4, 5)$, $(4, 6)$, etc., pertenecen a la relación h.

Ejemplo 26. La relación $j : \mathbb{N} \to \mathbb{N}$ dada por $j(n) = \sqrt{n}$ no es una función ya que no todo natural $n \in \mathbb{N}$ tiene una raíz cuadrada en $\mathbb{N}$.

Dos funciones $f : A \to B$ y $g : C \to D$ son *iguales* si tienen el mismo dominio $A = C$, mismo codominio $B = D$ y misma regla de correspondencia, *i.e.*, $f(x) = g(x)$ para toda $x \in A$.

EJERCICIO 34. Explique por qué las funciones $f : \mathbb{Z} \to \mathbb{N}$ y $g : \mathbb{Z} \to \mathbb{Z}$ dadas por $f(n) = n^2 + 1$ y $g(n) = n^2 + 1$ no son iguales.

Misma pregunta para las funciones $h : \mathbb{Z} \to \mathbb{Z}$ y $j : \mathbb{N} \to \mathbb{Z}$ dadas por $h(n) = 2n$ y $j(n) = 2n$.

EJERCICIO 35. Determine la imagen de cada una de las funciones siguientes:

$$\begin{aligned} f &: \mathbb{Z} \to \mathbb{Z} \quad \text{dada por } f(n) = n^2, \\ g &: \mathbb{Z} \to \mathbb{Z} \quad \text{dada por } g(n) = 3n, \\ h &: \mathbb{Z} \to \mathbb{Z} \quad \text{dada por } h(n) = 4n + 1. \end{aligned}$$

Clasificación de funciones. Hay varias clases de funciones que son importantes, aquí veremos algunas de ellas. Dada una función $f : A \to B$, diremos que:

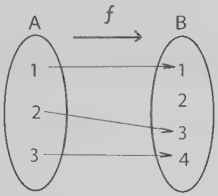
(•) $f : A \to B$ es *inyectiva* si siempre que $a \neq a'$ en A, se tiene que $f(a) \neq f(a')$ en B, es decir, puntos distintos en A tienen imágenes distintas en B.

Si llamamos q a la proposición lógica: $a = a'$ y llamamos p a la proposición lógica: $f(a) = f(a')$, la definición de que f sea inyectiva es la implicación: $\neg q \Rightarrow \neg p$. Si ahora recordamos que $(\neg q \Rightarrow \neg p) \equiv (p \Rightarrow q)$, entonces la definición de que f sea inyectiva es equivalente a decir que $f(a) = f(a')$ implica que $a = a'$.

(•) $f : A \to B$ es *suprayectiva* si todo elemento $b \in B$ es imagen de algún elemento $a \in A$, *i.e.*, $f(a) = b$. En otras palabras, $f : A \to B$ es suprayectiva si y sólo si la imagen de f es todo B, *i.e.*, $f(A) = B$.

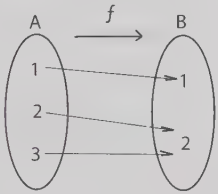
(•) $f : A \to B$ es *biyectiva* si es inyectiva y suprayectiva.

Ejemplo 27. La función



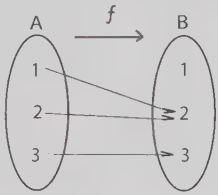
es inyectiva pero no es suprayectiva ya que el $2 \in B$ no es imagen de algún elemento de A.

Ejemplo 28. La función



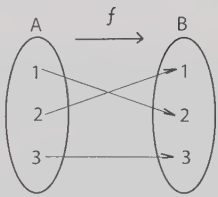
es suprayectiva pero no es inyectiva ya que $f(2) = 2 = f(3)$.

Ejemplo 29. La función



no es inyectiva ni suprayectiva.

Ejemplo 30. La función



es biyectiva.

Ejemplo 31. La función $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n$ es inyectiva pero no suprayectiva.

En efecto, es inyectiva ya que si $f(m) = f(n)$ entonces $2m = 2n$ y dividiendo entre 2 se sigue que $m = n$.

No es suprayectiva ya que sus imágenes son pares por lo que todos los impares de $\mathbb{N}$ no son imágenes bajo f de elementos de $\mathbb{N}$.

Ejemplo 32. La función $g : \mathbb{Z} \to \mathbb{Z}$ dada por $g(n) = n^2$ no es inyectiva ni suprayectiva.

En efecto, no es inyectiva ya que, por ejemplo, $g(-3) = 9 = g(3)$, y no es suprayectiva ya que las imágenes de g son enteros no negativos.

EJERCICIO 36. Considere las funciones siguientes:

$$\begin{aligned} f &: \mathbb{Z} \to \mathbb{Z} \quad \text{dada por } f(n) = n^2, \\ g &: \mathbb{Z} \to \mathbb{Z} \quad \text{dada por } g(n) = 3n, \\ h &: \mathbb{Z} \to \mathbb{Z} \quad \text{dada por } h(n) = 4n + 1. \end{aligned}$$

Determine cuáles son inyectivas y cuáles son suprayectivas.

EJERCICIO 37. Si $\mathbb{R}$ denota al conjunto de los números reales (de nuevo, si ya los vio en su curso de Cálculo), dado un número real $x \in \mathbb{R}$, denote por $[x] \in \mathbb{Z}$ al mayor entero $\leq x$.

(I) Calcule $[7.5]$, $[-2.4]$, $[\pi]$, $[-0.52]$.

(II) Muestre que la relación $f : \mathbb{R} \to \mathbb{Z}$ dada por $f(x) = [x]$ es una función y grafíquela.

(III) Demuestre que es suprayectiva pero no inyectiva.

EJERCICIO 38. Si A es cualquier conjunto no vacío, demuestre que la función identidad $\mathrm{id}_A : A \to A$ es biyectiva.

EJERCICIO 39. Si $A \subseteq B$ son conjuntos no vacíos, demuestre que la *función inclusión* $i : A \to B$ dada por $i(a) = a$, es inyectiva.

EJERCICIO 40. Sea $f : \mathbb{N} \to \mathbb{Z}$ la función dada por $f(n) = (-1)^n[n/2]$, donde $[\ ]$ es la función del ejercicio 37. Demuestre que f es biyectiva.

Composición de funciones. Si $f : A \to B$ y $g : B \to C$ son dos funciones (nótese que pedimos que el codominio de f, denotado $\mathrm{Cod}(f)$, sea igual al dominio de g, denotado $\mathrm{Dom}(f)$), se puede definir una nueva función de A en C, llamada la *composición* de f y g y denotada $g \circ f$, como sigue:

(1) $\mathrm{Dom}(g \circ f) = A$ y $\mathrm{Cod}(g \circ f) = C$.

(2) La regla de correspondencia de $g \circ f : A \to C$ es:

$$(g \circ f)(a) = g(f(a)),$$

donde notamos que para $a \in A$ se tiene que $f(a) \in B = \mathrm{Dom}(g)$ por lo que se puede calcular $g(f(a)) \in C$.

El diagrama siguiente ilustra la situación anterior:

$$A \xrightarrow{f} B \xrightarrow{g} C, \qquad A \xrightarrow{g \circ f} C$$

La composición $g \circ f$ se lee: f *compuesta con* g o también f *seguida de* g.

Ejemplo 33. Si $f : \mathbb{N} \to \mathbb{N}$ y $g : \mathbb{N} \to \mathbb{Z}$ están dadas por $f(n) = 2n + 1$ y $g(m) = m^2$, entonces la composición $g \circ f : \mathbb{N} \to \mathbb{Z}$ está dada por

$$(g \circ f)(a) = g(f(a)) = g(2n + 1) = (2n + 1)^2 = 4n^2 + 4n + 1.$$

Nótese que en este ejemplo la composición $f \circ g$ no está definida ya que $\mathrm{Cod}(g) = \mathbb{Z} \neq \mathbb{N} = \mathrm{Dom}(f)$.

Ejemplo 34. Si $f : \mathbb{N} \to \mathbb{Z}$ y $g : \mathbb{Z} \to \mathbb{N}$ están dadas por $f(m) = 3m + 2$ y $g(n) = n^2 + 1$, entonces la composición $g \circ f : \mathbb{N} \to \mathbb{N}$ está definida y

$$(g \circ f)(x) = g(f(x)) = g(3x + 2) = (3x + 2)^2 + 1 = 9x^2 + 12x + 5.$$

Nótese que en este ejemplo la composición $f \circ g : \mathbb{Z} \to \mathbb{Z}$ sí está definida y se tiene que:

$$(f \circ g)(x) = f(g(x)) = f(x^2 + 1) = 3(x^2 + 1) + 2 = 3x^2 + 5.$$

Este ejemplo nos muestra que aun cuando las composiciones $g \circ f$ y $f \circ g$ estén definidas, en general $g \circ f \neq f \circ g$, es decir, la composición de funciones en general no es una operación conmutativa.

Inversa de una función. Si $f : A \to B$ es una *función biyectiva*, entonces se puede definir una función $g : B \to A$ que "deshace" lo que f "hace", es decir, si $f(a) = b$ entonces $g(b) = a$. En efecto, como $f : A \to B$ es suprayectiva entonces todo $b \in B$ proviene de algún $a \in A$, *i.e.*, existe algún $a \in A$ tal que $b = f(a)$. Y como f es inyectiva entonces el $a \in A$ tal que $f(a) = b$ es único. Se puede entonces definir $g : B \to A$ mediante $g(b) = a$ si y sólo si $f(a) = b$. A la función g así definida se le llama una *inversa* de f. Observemos ahora que como $f : A \to B$ y $g : B \to A$, entonces se pueden hacer las dos composiciones $g \circ f : A \to A$ y $f \circ g : B \to B$; estas composiciones satisfacen que:

LEMA I.6. *Si $f : A \to B$ es una función biyectiva y $g : B \to A$ es una inversa de f, entonces:*

$$g \circ f = \mathrm{id}_A \qquad \text{y} \qquad f \circ g = \mathrm{id}_B .$$

Demostración. Esto es directo de la definición de g ya que, por ejemplo, si $a \in A$ y $f(a) = b$, entonces $(g \circ f)(a) = g(f(a)) = g(b) = a$, la última igualdad por definición de g. Se sigue que $(g \circ f)(a) = a = \mathrm{id}_A(a)$ y por lo tanto $g \circ f = \mathrm{id}_A$.

La otra igualdad se demuestra en forma similar. □

EJERCICIO 41. Si $f : A \to B$ es biyectiva y $g, h : B \to A$ son inversas de f, demuestre que $g = h$.

Se sigue que si $f : A \to B$ es biyectiva su inversa es *única* y la denotaremos por $f^{-1} : B \to A$. Así el lema anterior nos dice que:

$$f^{-1} \circ f = \mathrm{id}_A \qquad \text{y} \qquad f \circ f^{-1} = \mathrm{id}_B .$$

Ejemplo 35. La función $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(m) = m + 5$ es biyectiva y su inversa es $f^{-1}(n) = n - 5$. Para ver esto, escribamos $f(m) = n$, entonces $n = f(m) = m + 5$ y así, despejando a m, queda $m = n - 5$ de tal forma que se define $f^{-1}(n) = n - 5$. Se comprueba fácilmente que:

$$(f^{-1} \circ f)(n) = f^{-1}(f(n)) = f^{-1}(n + 5) = (n + 5) - 5 = n = \mathrm{id}_{\mathbb{Z}}(n)$$

y

$$(f \circ f^{-1})(n) = f(f^{-1}(n)) = f(n - 5) = (n - 5) + 5 = n = \mathrm{id}_{\mathbb{Z}}(n).$$

Ejemplo 36. La función $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 3x + 4$ es biyectiva y para calcular su inversa pongamos $y = f(x) = 3x + 4$; despejando x queda $3x = y - 4$ por lo que $x = \frac{1}{3}(y - 4)$. Se tiene así que

$$f^{-1}(x) = \frac{1}{3}(x - 4)$$

y se comprueba fácilmente que $f^{-1} \circ f = \mathrm{id}_{\mathbb{R}}$ y $f \circ f^{-1} = \mathrm{id}_{\mathbb{R}}$.

EJERCICIO 42. Demuestre que si $f : A \to B$ es biyectiva entonces $f^{-1} : B \to A$ también es biyectiva y por lo tanto tiene inversa; demuestre que $(f^{-1})^{-1} = f$.

Propiedades de las funciones inyectivas, suprayectivas y biyectivas. A continuación estudiamos el comportamiento de las funciones bajo la composición:

PROPOSICIÓN I.7. *Sean $f : A \to B$ y $g : B \to C$ funciones.*

(1) *Si f y g son inyectivas, entonces $g \circ f$ también lo es.*

(2) *Si f y g son suprayectivas, entonces $g \circ f$ también lo es.*

(3) *Si f y g son biyectivas, entonces $g \circ f$ también lo es.*

Demostración. (1) Para probar que $g \circ f : A \to C$ es inyectiva, supongamos que $(g \circ f)(a) = (g \circ f)(a')$; entonces $g(f(a)) = g(f(a'))$ y como g es inyectiva esta igualdad implica que $f(a) = f(a')$, pero como f es inyectiva, la última igualdad dice que $a = a'$.

(2) Para $g \circ f : A \xrightarrow{f} B \xrightarrow{g} C$, sea $c \in C$. Como g es suprayectiva existe $b \in B$ tal que $g(b) = c$. Para este $b \in B$ como f es suprayectiva existe $a \in A$ tal que $f(a) = b$. Se sigue que $c = g(b) = g(f(a)) = (g \circ f)(a)$ como se quería.

(3) Se sigue de (1) y (2). □

PROPOSICIÓN I.8. *Sean $f : A \to B$ y $g : B \to C$ funciones.*

(1) *Si $g \circ f : A \to C$ es inyectiva, entonces f también lo es.*

(2) *Si $g \circ f : A \to C$ es suprayectiva, entonces g también lo es.*

Demostración. (1) Supongamos que $f(a) = f(a')$. Aplicando g a esta igualdad se sigue que $g(f(a)) = g(f(a'))$ y como $g \circ f$ es inyectiva esto implica que $a = a'$.

(2) Sea $c \in C$. Como $g \circ f$ es suprayectiva, entonces existe $a \in A$ tal que $g(f(a)) = c$. Poniendo $b = f(a) \in B$ se tiene entonces que $g(b) = g(f(a)) = c$ y por lo tanto g es suprayectiva. □

COROLARIO I.9. *Sean $f : A \to B$ y $g : B \to A$ funciones tales que $g \circ f = \mathrm{id}_A$. Entonces f es inyectiva y g es suprayectiva.*

Demostración. Se sigue de la proposición anterior, ya que id_A es biyectiva. □

PROPOSICIÓN I.10. *Sea $f : A \to B$ una función. Entonces:*

(1) *Si f es inyectiva entonces para cualesquiera funciones $g_1, g_2 : M \to A$ se tiene que $f \circ g_1 = f \circ g_2$ implica que $g_1 = g_2$.*

(2) *Si f es suprayectiva entonces para cualesquiera funciones $g_1, g_2 : B \to M$ se tiene que $g_1 \circ f = g_2 \circ f$ implica que $g_1 = g_2$.*

Demostración. (1) Sólo se tiene que probar que g_1 y g_2 tienen la misma regla de correspondencia. Para esto, si $x \in M$, como $f \circ g_1 = f \circ g_2$ entonces $f(g_1(x)) = f(g_2(x))$ y como f es inyectiva esto implica que $g_1(x) = g_2(x)$ como se quería.

(2) De nuevo, sólo debemos probar que g_1 y g_2 tienen los mismos valores en toda $x \in B$. Para esto, si $x \in B$ como f es suprayectiva existe un $a \in A$ tal que $f(a) = x$ y aplicando g_1 a esta igualdad se sigue que $g_1(f(a)) = g_1(x)$; similarmente aplicando ahora g_2 a la igualdad anterior se tiene que $g_2(f(a)) = g_2(x)$. Y como $g_1 \circ f = g_2 \circ f$ por hipótesis, se sigue que

$$g_1(x) = g_1(f(a)) = g_2(f(a)) = g_2(x)$$

que es lo que se quería. □

La proposición anterior nos dice, de cierta manera, que si una función f es inyectiva entonces se puede *cancelar* de cualquier igualdad de la forma $f \circ g_1 = f \circ g_2$ para obtener que $g_1 = g_2$. Similarmente, cuando f es suprayectiva, se puede cancelar de cualquier igualdad $g_1 \circ f = g_2 \circ f$. Las definiciones siguientes capturan estas situaciones: si $f : A \to B$ es una función y si $f' : B \to A$ es otra función tal que $f' \circ f = \mathrm{id}_A$, entonces diremos que f' es *inversa izquierda* de f y que f es *inversa derecha* de f'.

Si sucediera que $f' \circ f = \mathrm{id}_A$ y $f \circ f' = \mathrm{id}_B$ diremos que f *inversa bilateral* de f' y que f' es *inversa bilateral* de f.

PROPOSICIÓN I.11. *Supongamos que $A \neq \emptyset$ y sea $f : A \to B$ una función. Entonces:*

(1) *f es inyectiva si y sólo si f tiene inversa izquierda.*

(2) *f es suprayectiva si y sólo si f tiene inversa derecha.*

Demostración. (1) ($\Leftarrow$): Supongamos que $f(x) = f(y)$. Como existe $f' : B \to A$ tal que $f' \circ f = \mathrm{id}_A$ entonces aplicando f' a la igualdad previa se sigue que $f'(f(x)) = f'(f(y))$, *i.e.,* $\mathrm{id}_A(x) = \mathrm{id}_A(y)$ por lo que $x = y$.

($\Rightarrow$): Suponemos ahora que f es inyectiva. Como $A \neq \emptyset$ podemos fijar un $a_0 \in A$. Entonces, dado $b \in B$ definimos

$$f'(b) = \begin{cases} a & \text{si } f(a) = b \\ a_0 & \text{si } b \notin f(A). \end{cases}$$

Nótese que si $f(a) = b$ entonces esta $a \in A$ es única porque f es inyectiva. Se sigue que f' es una función y además, para toda $a \in A$ se tiene que:

$$f' \circ f(a) = f'(f(a)) = a = \mathrm{id}_A(a),$$

i.e., $f' \circ f = \mathrm{id}_A$.

NOTA: Observe que existe una elección para el $a_0 \in A$ de tal forma que hay, en general, varias formas de definir la función f' que sea inversa izquierda de f, es decir, en general una función inyectiva f tiene varias inversas izquierdas.

(2) ($\Leftarrow$): Sea $b \in B$. Como existe $f' : B \to A$ tal que $f \circ f' = \mathrm{id}_B$, entonces $f \circ f'(b) = \mathrm{id}_B(b) = b$ y así, poniendo $a = f'(b) \in A$ se tiene que $f(a) = b$, *i.e.,* f es suprayectiva.

($\Rightarrow$): Supongamos ahora que f es suprayectiva. Entonces, para todo $b \in B$ existe algún $a \in A$ tal que $f(a) = b$. Fijo $b \in B$, escojamos un único $a \in A$ tal que $f(a) = b$ y definamos $f'(b) := a$. Entonces $(f \circ f')(b) = f(f'(b)) = f(a) = b = \mathrm{id}_B(b)$ y por lo tanto $f \circ f' = \mathrm{id}_B$ como se quería. □

NOTA: La segunda parte de esta demostración depende de la posibilidad de elegir para cada $b \in B$ un único $a \in A$ con la condición de que $f(a) = b$. Esto se puede hacer porque dado $b \in B$ el conjunto de los elementos $a \in A$ tal que $f(a) = b$ es no vacío ya que f es suprayectiva. Aquí parece intuitivamente claro que dada cualquier familia de conjuntos no vacíos uno siempre

puede elegir un miembro de cada conjunto de la familia. Sin embargo, esta afirmación tiene que pedirse de entrada en la teoría de conjuntos, es decir, tiene que incluirse como un axioma, al que se llama el *axioma de elección*. Si siente curiosidad acerca de los axiomas de la teoría de conjuntos, platique con su profesor, ¡aquí la curiosidad no mata al gato!

EJERCICIO 43. Dé ejemplos de funciones $f : A \to B$ y $g : B \to C$ tales que:

(I) f es inyectiva pero $g \circ f$ no lo es.

(II) g es suprayectiva pero $g \circ f$ no lo es.

(III) f es inyectiva y g es suprayectiva pero $g \circ f$ no es inyectiva ni suprayectiva.

(IV) f no es suprayectiva y g no es inyectiva pero $g \circ f$ es biyectiva.

EJERCICIO 44. Sean $f : A \to B$ y $g : B \to C$ funciones tales que ambas tienen inversas izquierdas. Demuestre que $g \circ f$ tiene inversa izquierda.

EJERCICIO 45. Sea $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n^2$.

(I) Exhiba dos inversas izquierdas de f.

(II) Muestre que f no tiene inversa derecha.

EJERCICIO 46. Sean $f : \mathbb{Z} \to \mathbb{Z}$ y $g : \mathbb{Z} \to \mathbb{Z}$ dadas por $f(n) = 2n$ y $g(n) = [n/2]$. Muestre que $g \circ f = \mathrm{id}_{\mathbb{Z}}$ pero $f \circ g \neq \mathrm{id}_{\mathbb{Z}}$.

EJERCICIO 47. Suponga que A y B son no vacíos y sea $f : A \to B$ una función que tiene inversa izquierda g e inversa derecha h.

(I) Demuestre que $g = h$.

(II) Concluya que f es biyectiva.

EJERCICIO 48. Demuestre que cualquier función $f : A \to B$ se puede descomponer como $f = g \circ h$ con g inyectiva y h suprayectiva. *Sugerencia*: ponga $M = f(A) \subseteq B$.

EJERCICIO 49. Sea $f : A \to B$ una función. Si $X \subseteq A$ es cualquier subconjunto, la *imagen de X bajo f* es el conjunto

$$f(X) := \{f(x) \in B \ : \ x \in X\} \subseteq B.$$

(I) Demuestre que $f(\emptyset) = \emptyset$.

(II) Si $X_1, X_2 \subseteq A$, demuestre que $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.

(III) Si $X_1, X_2 \subseteq A$, demuestre que $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.

(IV) Dé un ejemplo donde no se cumpla la igualdad en el ejercicio anterior.

(V) Si $X_1, X_2 \subseteq A$, demuestre que $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ si y sólo si f es inyectiva.

(VI) Si $\{X_\alpha\}$ es una familia de subconjuntos de A, demuestre que

$$f\left(\bigcup_\alpha X_\alpha\right) = \bigcup_\alpha f(X_\alpha).$$

(VII) Si $\{X_\alpha\}$ es una familia de subconjuntos de A, demuestre que

$$f\left(\bigcap_\alpha X_\alpha\right) \subseteq \bigcap_\alpha f(X_\alpha).$$

EJERCICIO 50. Sea $f : A \to B$ una función. Si $Y \subseteq B$ es un subconjunto, se define la *imagen inversa o preimagen de Y bajo f* como

$$f^{-1}(Y) := \{x \in A \ : \ f(x) \in Y\} \subseteq A.$$

(I) Demuestre que $f^{-1}(\emptyset) = \emptyset$.

(II) Si $Y_1, Y_2 \subseteq B$, demuestre que $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

(III) Si $Y_1, Y_2 \subseteq B$, demuestre que $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

(IV) Note que la imagen inversa se comporta mejor que la imagen directa.

(V) $f^{-1}(Y)^c = f^{-1}(Y^c)$.

(VI) Si $\{Y_\alpha\}$ es una familia de subconjuntos de B, demuestre que

$$f^{-1}\left(\bigcup_\alpha Y_\alpha\right) = \bigcup_\alpha f^{-1}(Y_\alpha).$$

(VII) Si $\{Y_\alpha\}$ es una familia de subconjuntos de B, demuestre que

$$f^{-1}\left(\bigcap_\alpha Y_\alpha\right) = \bigcap_\alpha f^{-1}(Y_\alpha).$$

EJERCICIO 51. Sean $f : A \to B$ una función, $X \subseteq A$ y $Y \subseteq B$ conjuntos. Demuestre que:

(I) $f(f^{-1}(Y)) \subseteq Y$.

(II) $f(f^{-1}(Y)) = Y$ si y sólo si f es suprayectiva.

(III) $X \subseteq f^{-1}(f(X))$.

(IV) $X = f^{-1}(f(X))$ si y sólo si f es inyectiva.

(V) $f(X)^c = f(X^c)$ si y sólo si f es biyectiva.

EJERCICIO 52. Si X es un conjunto y $A \subseteq X$ es un subconjunto, se define la *función característica* de A, $c_A : X \to \{0, 1\}$, mediante

$$c_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A. \end{cases}$$

(I) Si A, B son subconjuntos de X, demuestre que $c_{A\cap B} = c_A \cdot c_B$.

(II) Si A, B son subconjuntos de X, demuestre que $c_{A\cup B} = c_A + c_B - c_{A\cap B}$.

(III) Si A^c es el complemento de A, demuestre que $c_{A^c} = 1 - c_A$.

EJERCICIO 53. Si $f : Y \to Y$ es una función suprayectiva, para cada $y \in Y$ considere la imagen inversa de $\{y\} \subseteq Y$, $f^{-1}\{y\} \subseteq X$ y demuestre que la familia de imágenes inversas $f^{-1}\{y\}$, variando $y \in Y$, forma una partición de X.

II. LOS NÚMEROS NATURALES

Los enteros positivos $1, 2, 3, \ldots$, a los que llamamos *números naturales*, de alguna forma son los primeros números que se nos aparecen *en forma natural* al *contar* o al *ordenar* los elementos de algunos conjuntos. De manera informal podemos pensar que, para ordenar un conjunto tenemos que elegir un primer elemento, al que podemos llamar el *número uno*, denotado por 1. Después, debemos tener un mecanismo o método que nos diga cuál es el *número siguiente*. Es decir, necesitamos pedir que nuestro conjunto de números naturales debe contener al número 1 y debe existir una función s del conjunto de los naturales en sí mismo que asigne a un número natural dado el *número que le sigue*, de tal forma que el número que le sigue al 1 es el 2, el que le sigue al 2 es el 3, etc. Para estudiar los números naturales, el enfoque que usaremos es *axiomático* y esencialmente se debe a Giuseppe Peano. La idea del método axiomático es listar una serie de propiedades de los números naturales, a las que llamamos *axiomas* o *postulados*, y tener estos axiomas como definitorios de estos números. Los *axiomas de Peano* para los números naturales, cuyo conjunto denotaremos con $\mathbb{N}$, son los siguientes:

Axioma 1. El conjunto $\mathbb{N}$ contiene a un elemento al que denotamos con 1.

Axioma 2. Existe una función $s : \mathbb{N} \to \mathbb{N}$ a la que llamamos *función sucesor*, que a cada número natural $n \in \mathbb{N}$ le asocia su sucesor $s(n) \in \mathbb{N}$.

Axioma 3. La función $s : \mathbb{N} \to \mathbb{N}$ es *inyectiva*.

Axioma 4. El $1 \in \mathbb{N}$ no es sucesor de un número natural.

Axioma 5 (Axioma de inducción). Si $M \subseteq \mathbb{N}$ es un subconjunto tal que:

(i) $1 \in M$.

(ii) $\forall n \in M$ se tiene que $s(n) \in M$,

entonces $M = \mathbb{N}$.

La idea detrás de estos axiomas es capturar lo que sentimos que son los números naturales, por ejemplo, el primer axioma nos dice que $1 \in \mathbb{N}$ y el segundo axioma nos dice entonces que $s(1) = 2 \in \mathbb{N}$ y de nuevo $s(2) = 3 \in \mathbb{N}$, etc. El tercer axioma nos dice que números distintos deben tener sucesores distintos y el cuarto axioma nos dice que 1 es el primer número natural. El axioma de inducción formalmente nos permite definir y probar propiedades de los naturales. Las propiedades axiomáticas que hemos listado corresponden a la concepción intuitiva que tenemos de los números naturales y al aceptar estos axiomas, de alguna forma también estamos aceptando la existencia de un conjunto de números que los satisfacen. Sin embargo, la existencia de este conjunto no se puede deducir de los 5 axiomas listados arriba usando los principios generales de la teoría de conjuntos descritos en el capítulo anterior y, consecuentemente, la existencia de un sistema de números que satisfacen los axiomas de Peano debe también ser postulada:

Axioma 0 (Existencia de $\mathbb{N}$). Existe un conjunto $\mathbb{N}$ que satisface los axiomas de Peano.

Uno de los objetivos importantes será probar la *unicidad* del conjunto de los números naturales, pero primero veamos que si alguno de los axiomas de Peano no se satisface, esta unicidad no sería cierta. Para comenzar, observamos que los primeros dos axiomas sólo nos dicen que hay un elemento (el 1) y una función $s : \mathbb{N} \to \mathbb{N}$, así, los axiomas que podemos eliminar son el 3, 4 y 5:

- Un ejemplo de un conjunto que no satisface el axioma 4 es el conjunto $N = \{1'\}$ junto con la función $s' : N \to N$ dada por $s'(1') := 1'$. ¡Ciertamente no queremos que este N sea el conjunto de números naturales!

- Un ejemplo de un conjunto que no satisface el axioma 3 es el conjunto $N = \{1', 2'\}$, con $1' \neq 2'$, junto con la función $s' : N \to N$ dada por $s'(1') := 2'$ y $s'(2') := 2'$. ¡Tampoco queremos que este N sea el conjunto de números naturales!

- Los dos ejemplos anteriores son "muy chicos" y por eso no nos sirven. Para dar un ejemplo de un conjunto N y una función sucesor $s' : N \to N$ que no satisfagan el axioma 5 debemos primero tener un elemento

$1' \in N$ de tal forma que N también debe contener al menos a los elementos $s'(1')$, $s'(s'(1'))$, $s'(s'(s'(1')))$, etc., observando que, como debe ahora de satisfacerse el axioma 4, entonces $1' \neq s'(1')$. También, como el axioma 3 es válido, si sucediera que $s'(s'(1')) = s'(1')$ entonces se tendría que $s'(1') = 1'$, en contradicción con el axioma 4. En forma similar se prueba que todos los elementos $s'(s'(\cdots s'(1')\cdots)$ de N son distintos entre sí. Consideremos ahora otro elemento z distinto de los elementos $s'(1')$, $s'(s'(1'))$, $s'(s'(s'(1')))$,..., y consideremos elementos nuevos $s'(z)$, $s'(s'(z))$, $s'(s'(s'(z)))$, etc. (distintos de los anteriores); sea

$$N = \{1', z, s'(1'), s'(z), s'(s'(1')), s'(s'(z)), \ldots\}.$$

Claramente N satisface todos los axiomas de Peano excepto el axioma 5, ya que el conjunto

$$M = \{1', s'(1'), s'(s'(1')), \ldots\} \subseteq N$$

es tal que $1' \in M$ y para todo $m \in M$ se tiene que $s'(m) \in M$; sin embargo, $M \neq N$.

Antes de comenzar a estudiar formalmente el conjunto $\mathbb{N}$, unas palabras de precaución: estamos tan familiarizados con los números naturales que sus propiedades nos parecen obvias; sin embargo, con el enfoque formal que ahora tenemos todas estas propiedades "obvias" deben ser probadas usando los axiomas de Peano y las propiedades de lógica, conjuntos, relaciones y funciones que ya conocemos. Para ilustrar esto probaremos los dos resultados siguientes que nos serán útiles después. A resultados que se usarán para probar otras proposiciones más importantes se les suele llamar *lemas.*

LEMA II.1. *Si $a \in \mathbb{N}$ entonces $s(a) \neq a$.*

Demostración. Sea $M = \{a \in \mathbb{N} : s(a) \neq a\}$. Mostraremos que $M = \mathbb{N}$ usando el axioma de inducción. En efecto,

(I) $1 \in M$ ya que por el axioma 4, $1 \neq s(n)$ para todo $n \in \mathbb{N}$.

(II) Supongamos ahora que $n \in M$ (llamaremos a esto la *hipótesis de inducción*). Queremos mostrar que $s(n) \in M$ (llamaremos a esto el *paso inductivo*). En efecto, la hipótesis nos dice que $s(n) \neq n$ y como s es inyectiva por el axioma 3, entonces $s(s(n)) \neq s(n)$ y así, por definición de M se sigue que $s(n) \in M$.

Hemos así comprobado las condiciones (I) y (II) del axioma de inducción por lo que se tiene que $M = \mathbb{N}$. □

Observación. En general, el patrón de la demostración por inducción del lema anterior se repetirá, con las variaciones necesarias, siempre que queramos probar alguna afirmación que involucre a todos los números naturales. La parte (I) la llamaremos la *base de la inducción*, la parte (II) la llamaremos el *paso inductivo*, y la hipótesis de (II) se llamará la *hipótesis de inducción.*

LEMA II.2. *Si $a \in \mathbb{N} - \{1\}$, entonces existe un único $n \in \mathbb{N}$ tal que $s(n) = a$. En otras palabras, la función $s : \mathbb{N} \to \mathbb{N} - \{1\}$ es suprayectiva.*

Demostración. Sea

$$M = \{a \in \mathbb{N} - \{1\} \ : \text{ existe un único } n \in \mathbb{N} \text{ tal que } s(n) = a\} \cup \{1\}.$$

Entonces,

(I) $1 \in M$ (por eso le unimos el conjunto $\{1\}$).

(II) Supongamos que $a \in M$ y que $a \neq 1$. Queremos probar que $s(a) \in M$. Para esto observemos que por hipótesis de inducción existe un único $n \in \mathbb{N}$ tal que $a = s(n) \in \mathbb{N}$ y por lo tanto $s(a) = s(s(n)) \in \mathbb{N}$. La unicidad es por la inyectividad de s. Se sigue que $s(a) \in M$ y así, por el axioma de inducción se tiene que $M = \mathbb{N}$. □

Para finalizar esta sección, probaremos la unicidad del sistema de números naturales. Comenzamos precisando el significado de esta unicidad: a un conjunto $\mathbb{N}$ junto con el elemento $1 \in \mathbb{N}$ y la función sucesor $s : \mathbb{N} \to \mathbb{N}$ que satisfacen los axiomas de Peano, lo llamaremos un *sistema de Peano* y lo denotaremos por la terna $(\mathbb{N}, 1, s)$. El sentido que le daremos al concepto de *unicidad* de un sistema de Peano es el siguiente: para cualesquiera dos de ellos, los conjuntos correspondientes son biyectivos mediante una biyección que lleva el elemento *uno* de un sistema al *uno* del otro sistema y que además lleva al sucesor de un elemento de un sistema al sucesor del elemento correspondiente del otro sistema. Así, mediante esta biyección pensaremos que los dos sistemas son indistinguibles. Esto se precisa como sigue:

Supongamos que $(\mathbb{N}, 1, s)$ y $(\mathbb{N}', 1', s')$ son sistemas de Peano. Diremos que estos dos sistemas de Peano son *isomorfos* (esto significa que son "indistinguibles" o que tienen la "misma forma") si existe una función biyectiva $F : \mathbb{N} \to \mathbb{N}'$ tal que:

(I) $F(1) = 1'$, *i.e.*, F respeta los elementos distinguidos 1 y $1'$.

(II) Para toda $x \in \mathbb{N}$ se tiene que $F(s(x)) = s'(F(x))$, *i.e.*, $F \circ s = s' \circ F$. (Decimos que F *respeta* las funciones sucesor).

Así, el teorema que queremos probar es:

TEOREMA II.3 (Unicidad del sistema de Peano). *Cualesquiera dos sistemas de Peano son isomorfos.*

Demostración. Supongamos que $(\mathbb{N}, 1, s)$ y $(\mathbb{N}', 1', s')$ son sistemas de Peano. Queremos definir una función $F : \mathbb{N} \to \mathbb{N}'$ que satisfaga las condiciones (I) y (II) anteriores y que además sea biyectiva. La definición de F se hará por inducción:

Primero se define $F(1) := 1'$. (De tal forma que la condición (I) se satisface.)

Supongamos que $F(n) \in \mathbb{N}'$ ya ha sido definido para $n \in \mathbb{N}$. Entonces, se define $F(s(n)) := s'(F(n))$. (De tal forma que la condición (II) se satisface, por definición.)

Mostraremos ahora que F es *suprayectiva* por inducción en $\mathbb{N}'$: sea

$$A' = \{y \in \mathbb{N}' \ : \ \text{existe } x \in \mathbb{N} \text{ tal que } F(x) = y\} = F(\mathbb{N}).$$

Para probar que F es suprayectiva debemos mostrar que $A' = \mathbb{N}'$, y esto lo haremos por inducción en $\mathbb{N}'$.

Claramente $1' \in A'$ ya que $F(1) = 1'$.

Supongamos ahora que $y \in A'$, es decir, que existe $x \in \mathbb{N}$ tal que $y = F(x)$. Entonces,

$$\begin{aligned} s'(y) &= s'(F(x)) \\ &= F(s(x)) \qquad \text{por definición de } F, \end{aligned}$$

con $s(x) \in \mathbb{N}$. Se sigue que $s'(y) \in A'$ y por lo tanto $A' = \mathbb{N}'$ por inducción en $(\mathbb{N}', 1', s')$, habiendo mostrado así que F es suprayectiva.

Mostraremos ahora que F es *inyectiva* por inducción en $\mathbb{N}$: sea

$$A = \{x \in \mathbb{N} \ : \ \forall z \in \mathbb{N},\ F(z) = F(x) \Rightarrow z = x\}.$$

Para probar que F es inyectiva basta mostrar que $A = \mathbb{N}$, y esto lo haremos por inducción en $\mathbb{N}$.

Mostraremos primero que $1 \in A$, *i.e.*, mostraremos que si $F(z) = 1'$, entonces $z = 1$. En efecto, si existiera $z \in \mathbb{N}$ tal que $F(z) = 1'$ con $z \neq 1$, entonces $z \in \mathbb{N} - \{1\}$ y como, por el lema (II.2), $s : \mathbb{N} \to \mathbb{N} - \{1\}$ es suprayectiva, entonces existe un $w \in \mathbb{N}$ tal que $z = s(w)$, y por lo tanto

$$\begin{aligned} 1' &= F(z) \\ &= F(s(w)) \\ &= s'(F(w)) \quad \text{por definición de } F, \end{aligned}$$

por lo que $1'$ es sucesor del elemento $F(w) \in \mathbb{N}'$, en contradicción con el axioma 4 del sistema $(\mathbb{N}', 1', s')$. Se sigue que $1 \in A$.

Supongamos ahora que $x \in A$, *i.e.*, si $F(z) = F(x)$ entonces $z = x$ (para cualquier $z \in \mathbb{N}$). Mostraremos que $s(x) \in A$, *i.e.*, probaremos que si $F(w) = F(s(x))$, entonces $w = s(x)$ (para cualquier $w \in \mathbb{N}$). En efecto, como

$$F(w) = F(s(x)) = s'(F(x)), \tag{1}$$

entonces w no puede ser igual a 1, ya que esto estaría en contradicción con el axioma 4. Así, $w \neq 1$, y por el lema (II.2), $w = s(z)$ para un $z \in \mathbb{N}$. Por lo tanto

$$F(w) = F(s(z)) = s'(F(z)), \tag{2}$$

y de (1) y (2) se sigue que $s'(F(x)) = s'(F(z))$. Pero como s' es inyectiva, por el axioma 3, la última igualdad implica que $F(x) = F(z)$; pero, por la hipótesis de inducción esto último implica que $z = x$. Se sigue que $w = s(z) = s(x)$, como se quería probar. □

II.1 Operaciones en $\mathbb{N}$

Como todos sabemos, los números naturales se pueden sumar y multiplicar y a continuación definimos formalmente estas operaciones en $\mathbb{N}$ usando el axioma de inducción y diremos que estas definiciones son *inductivas* o *recursivas*:

La suma en $\mathbb{N}$. Fijemos un $a \in \mathbb{N}$.

(I) Primero definimos la suma con 1:

$$a + 1 := s(a).$$

(II) Suponiendo ya definida la suma $a + b$ para $b \in \mathbb{N}$, se define:

$$a + s(b) := s(a + b).$$

Por el axioma de inducción hemos así definido la suma $a + b$ en todo $\mathbb{N}$. Para probar las propiedades esperadas de la suma nos será muy útil el lema siguiente:

LEMA II.4. *Si $a, b \in \mathbb{N}$, entonces $s(a) + b = s(a + b)$.*

Demostración. Fijemos $a \in \mathbb{N}$ y sea $M = \{b \in \mathbb{N} \ : \ s(a) + b = s(a + b)\}$. Entonces:

(I) $1 \in M$ ya que

$$\begin{aligned} s(a) + 1 &= s(s(a)) && \text{por la definición (I) de suma} \\ &= s(a + 1) && \text{por la definición (I) de suma.} \end{aligned}$$

(II) Supongamos que $b \in M$. Queremos probar que $s(b) \in M$. En efecto, por hipótesis de inducción $s(a) + b = s(a + b)$ y así

$$\begin{aligned} s(a) + s(b) &= s(s(a) + b) && \text{por la definición (II) de suma} \\ &= s(s(a + b)) && \text{por hipótesis de inducción} \\ &= s(a + s(b)) && \text{por la definición (II) de suma} \end{aligned}$$

y así, por definición de M se sigue que $s(b) \in M$. Por el axioma de inducción se tiene que $M = \mathbb{N}$. □

La *conmutatividad* de la suma en $\mathbb{N}$ la probaremos en dos pasos:

LEMA II.5. *Para todo $a \in \mathbb{N}$ se tiene que $a + 1 = 1 + a$.*

Demostración. Sea $M = \{a \in \mathbb{N} \ : \ a + 1 = 1 + a\}$. Entonces:

(I) $1 \in M$ ya que $1 + 1 = 1 + 1$.

(II) Supongamos que $a \in M$. Queremos probar que $s(a) \in M$. En efecto,

$$\begin{aligned} s(a) + 1 &= s(a + 1) && \text{por el lema (II.4)} \\ &= s(1 + a) && \text{por hipótesis de inducción} \\ &= 1 + s(a) && \text{por la definición (II) de suma.} \end{aligned}$$ □

PROPOSICIÓN II.6 (Conmutatividad de la suma en $\mathbb{N}$). *Para todo $a, b \in \mathbb{N}$ se tiene que $a + b = b + a$.*

Demostración. Fijemos $a \in \mathbb{N}$ y sea $M = \{b \in \mathbb{N} \ : \ a + b = b + a\}$. Entonces:

(I) $1 \in M$ por el lema previo.

(II) Supongamos que $b \in M$. Queremos probar que $s(b) \in M$. En efecto,

$$\begin{aligned} a + s(b) &= s(a + b) && \text{por la definición (II) de suma} \\ &= s(b + a) && \text{por hipótesis de inducción} \\ &= s(b) + a && \text{por el lema (II.4).} \end{aligned}$$ □

PROPOSICIÓN II.7 (Asociatividad de la suma en $\mathbb{N}$). *Para todo $a, b, c \in \mathbb{N}$ se tiene que $a + (b + c) = (a + b) + c$.*

Demostración. Sea $M = \{c \in \mathbb{N} \ : \ a + (b + c) = (a + b) + c \ \ \forall a, b \in \mathbb{N}\}$. Entonces:

(I) $1 \in M$ ya que

$$\begin{aligned} a + (b + 1) &= a + s(b) && \text{por definición de suma} \\ &= s(a + b) && \text{por definición de suma} \\ &= (a + b) + 1 && \text{por definición de suma.} \end{aligned}$$

(II) Supongamos que $c \in M$, *i.e.*, que $a + (b + c) = (a + b) + c$. Entonces

$$\begin{aligned} a + (b + s(c)) &= a + s(b + c) && \text{por definición de suma} \\ &= s(a + (b + c)) && \text{por definición de suma} \\ &= s((a + b) + c) && \text{por hipótesis de inducción} \\ &= (a + b) + s(c) && \text{por definición de suma,} \end{aligned}$$

i.e., $s(c) \in M$. □

PROPOSICIÓN II.8 (Ley de cancelación para la suma). *Sean $a, b, c \in \mathbb{N}$ y supongamos que $a + c = b + c$, entonces $a = b$.*

Demostración. Fijemos $a, b \in \mathbb{N}$ y sea $M = \{c \in \mathbb{N} : a+c = b+c \Rightarrow a = b\}$. Entonces

(I) $1 \in M$ ya que si $a+1 = b+1$ entonces $s(a) = s(b)$ y como s es inyectiva entonces $a = b$.

(II) Supongamos que $c \in M$, *i.e.*, que $a + c = b + c \Rightarrow a = b$. Entonces

$$\begin{aligned} a + s(c) = b + s(c) &\Rightarrow s(a + c) = s(b + c) && \text{por definición de suma} \\ &\Rightarrow a + c = b + c && \text{porque } s \text{ es inyectiva} \\ &\Rightarrow a = b && \text{por hipótesis de inducción,} \end{aligned}$$

i.e., $s(c) \in M$. □

El producto en $\mathbb{N}$. Fijemos un $a \in \mathbb{N}$.

(I) Primero definimos el producto con 1:

$$a \cdot 1 := a.$$

(II) Suponiendo ya definido el producto $a \cdot b$ para $b \in \mathbb{N}$, se define:

$$a \cdot s(b) := a \cdot b + a.$$

Por el axioma de inducción hemos así definido el producto ab en todo $\mathbb{N}$. Para probar las propiedades esperadas del producto nos será muy útil el lema siguiente:

LEMA II.9. *Si $a, b \in \mathbb{N}$, entonces $s(a)b = ab + b$.*

Demostración. Fijemos $a \in \mathbb{N}$ y sea $M = \{b \in \mathbb{N} : s(a)b = ab + b\}$. Entonces:

(I) $1 \in M$ ya que

$$\begin{aligned} s(a) \cdot 1 &= s(a) && \text{por la definición (I) del producto} \\ &= a + 1 && \text{por la definición (I) de suma} \\ &= a \cdot 1 + 1 && \text{por definición del producto.} \end{aligned}$$

(II) Supongamos que $b \in M$, *i.e.*, que $s(a)b = ab + b$. Entonces

$$\begin{aligned} s(a)s(b) &= s(a)b + s(a) && \text{por definición del producto} \\ &= (ab + b) + s(a) && \text{por hipótesis de inducción} \\ &= ab + (b + s(a)) && \text{por la asociatividad de la suma} \\ &= ab + s(b + a) && \text{por definición de suma} \\ &= ab + (s(b) + a) && \text{por el lema (II.4)} \\ &= (ab + a) + s(b) && \text{asociatividad y conmutatividad de la suma} \\ &= as(b) + s(b) && \text{por definición del producto,} \end{aligned}$$

y así, por definición de M se sigue que $s(b) \in M$. □

La *conmutatividad* del producto en $\mathbb{N}$ la probaremos en dos pasos:

LEMA II.10. *Para todo $a \in \mathbb{N}$ se tiene que $a \cdot 1 = 1 \cdot a$.*

Demostración. Sea $M = \{a \in \mathbb{N} \,:\, 1 \cdot a = a\}$. Entonces:

(I) $1 \in M$ ya que $1 \cdot 1 = 1$ por definición del producto.

(II) Supongamos que $a \in M$, *i.e.*, que $1 \cdot a = a$. Entonces

$$\begin{aligned} 1 \cdot s(a) &= 1 \cdot a + 1 && \text{por definición de producto} \\ &= a + 1 && \text{por hipótesis de inducción} \\ &= s(a) && \text{por definición de suma.} \end{aligned}$$ □

PROPOSICIÓN II.11 (Conmutatividad del producto en $\mathbb{N}$). *Para todo $a, b \in \mathbb{N}$ se tiene que $ab = ba$.*

Demostración. Fijemos $a \in \mathbb{N}$ y sea $M = \{b \in \mathbb{N} \,:\, ab = ba\}$. Entonces:

(I) $1 \in M$ por el lema previo.

(II) Supongamos que $b \in M$, *i.e.*, que $ab = ba$. Entonces

$$\begin{aligned} as(b) &= ab + a && \text{por definición de producto} \\ &= ba + a && \text{por hipótesis de inducción} \\ &= s(b)a && \text{por el lema (II.9).} \end{aligned}$$ □

PROPOSICIÓN II.12 (Distributividad). *Para todo* $a, b, c \in \mathbb{N}$ *se tiene que*

$$a(b+c) = ab + ac.$$

Demostración. Sea $M = \{c \in \mathbb{N} \ : \ a(b+c) = ab + ac \ \ \forall a, b \in \mathbb{N}\}$. Entonces

(I) $1 \in M$ porque:

$$\begin{aligned} a(b+1) &= as(b) && \text{por definición de suma} \\ &= ab + a && \text{por definición de producto} \\ &= ab + a \cdot 1 && \text{por definición de producto.} \end{aligned}$$

(II) Supongamos que $c \in M$, *i.e.*, que $a(b+c) = ab + ac$. Entonces

$$\begin{aligned} a(b+s(c)) &= as(b+c) && \text{por definición de suma} \\ &= a(b+c) + a && \text{por definición de producto} \\ &= (ab+ac) + a && \text{por hipótesis de inducción} \\ &= ab + (ac + a) && \text{por asociatividad de la suma} \\ &= ab + as(c) && \text{por definición de producto.} \end{aligned}$$

Se sigue que $s(c) \in M$. □

PROPOSICIÓN II.13 (Asociatividad del producto en $\mathbb{N}$). *Para todo* $a, b, c \in \mathbb{N}$ *se tiene que* $a(bc) = (ab)c$.

Demostración. Sea $M = \{c \in \mathbb{N} \ : \ a(bc) = (ab)c \ \ \forall a, b \in \mathbb{N}\}$. Entonces:

(I) $1 \in M$ ya que

$$\begin{aligned} a(b \cdot 1) &= ab && \text{por definición de producto} \\ &= (ab) \cdot 1 && \text{por definición de producto.} \end{aligned}$$

(II) Supongamos que $c \in M$, *i.e.*, que $a(bc) = (ab)c$. Entonces

$$\begin{aligned} (ab)s(c) &= (ab)c + ab && \text{por definición de producto} \\ &= a(bc) + ab && \text{por hipótesis de inducción} \\ &= a(bc + b) && \text{por distributividad} \\ &= a(bs(c)) && \text{por definición de producto,} \end{aligned}$$

i.e., $s(c) \in M$. □

II.2 El orden en $\mathbb{N}$

La idea que nos llevó a los axiomas de Peano para los números naturales es la noción de *sucesor* como una función $s : \mathbb{N} \to \mathbb{N}$ que asigna a cada natural $m \in \mathbb{N}$ el número $s(m) \in \mathbb{N}$ que le sigue. Si $n = s(m)$ diremos que m *precede* a n y lo denotamos por $m < n = s(m)$. En general, dados dos naturales $a, b \in \mathbb{N}$, diremos que a *precede* a b si existen naturales n_1, n_2,..., n_k tales que:

$$(*) \qquad b = s(n_1), n_1 = s(n_2), \ldots, n_k = s(a)$$

y lo denotamos mediante $a < b$. Recordemos ahora que, por definición de *suma* en $\mathbb{N}$, las igualdades $(*)$ nos dicen que:

$$b = s(n_1) = n_1{+}1 = s(n_2){+}1 = (n_2{+}1){+}1 = (s(n_3){+}1){+}1{+}1 = \cdots = a{+}k,$$

de tal forma que $a < b$ quiere decir que $b = a + k$ con $k \in \mathbb{N}$. Formalmente podemos entonces definir: si $a, b \in \mathbb{N}$ diremos que $a < b$ (se lee: a es menor que b) si $\exists n \in \mathbb{N}$ tal que $b = a + n$. También usaremos la notación $a > b$ (se lee: a es mayor que b) para indicar que $b < a$.

Proposición II.14 (Transitividad del orden). *Si $a < b$ y $b < c$ en $\mathbb{N}$, entonces $a < c$.*

Demostración. La hipótesis $a < b$ quiere decir que $\exists n \in \mathbb{N}$ tal que $b = a + n$ y la hipótesis $b < c$ quiere decir que $\exists m \in \mathbb{N}$ tal que $c = b + m$. Entonces

$$c = b + m = (a + n) + m = a + (m + n) \qquad \text{con } m + n \in \mathbb{N}$$

y así $a < c$. □

Para la propiedad siguiente necesitaremos:

Lema II.15. *Para todo $a, b \in \mathbb{N}$ se tiene que $a \neq a + b$.*

Demostración. Fijemos $b \in \mathbb{N}$ y sea $M = \{a \in \mathbb{N} \ : \ a \neq a + b\}$. Entonces

(i) $1 \in M$ ya que $1 \neq s(n)$ para todo $n \in \mathbb{N}$ por el axioma 4. Se sigue que $1 \neq n + 1$ para todo $n \in \mathbb{N}$ por definición de suma y por lo tanto $1 \neq 1 + n$ por la conmutatividad de la suma, *i.e.*, $1 \in M$.

(ii) Supongamos que $a \in M$, *i.e.*, que $a \neq a + b$. Entonces $s(a) \neq s(a + b)$ ya que s es inyectiva. Pero por el lema (II.4) $s(a + b) = s(a) + b$ y por lo tanto $s(a) \neq s(a) + b$, *i.e.*, $s(a) \in M$. □

PROPOSICIÓN II.16 (Tricotomía). *Si $a, b \in \mathbb{N}$, entonces se cumple exactamente una de las posibilidades siguientes:*

(1) $a = b$

(2) $a < b$

(3) $b < a$.

Demostración. Por el lema previo $\forall c, n \in \mathbb{N}$ se tiene que $c + n \neq c$. Se sigue que los casos (1) y (2) son incompatibles ya que $a < b$ quiere decir que $\exists n \in \mathbb{N}$ tal que $b = a + n$ y por lo tanto $b = a + n \neq a$. Similarmente (1) y (3) son incompatibles. También (2) y (3) son incompatibles ya que si $b = a + n$ y $a = b + m$, entonces

$$b = a + n = (b + m) + n = b + (m + n)$$

con $m + n \in \mathbb{N}$, en contradicción con el lema previo. Así, a lo más uno de los casos (1), (2), (3) es verdadero.

Fijemos ahora $a \in \mathbb{N}$ y sea $M = \{b \in \mathbb{N} \ : \ (1), (2) \text{ o } (3) \text{ es cierta}\}$. Usando inducción mostraremos que $M = \mathbb{N}$. En efecto,

(I) $1 \in M$ ya que como $a \in \mathbb{N}$ entonces $a = 1$ o $a = s(c)$ para algún $c \in \mathbb{N}$ por el lema (II.2). Así $a = 1 = b$ o $a = s(c) = c + 1 = 1 + c$ con $c \in \mathbb{N}$ por lo que $1 < a$. Es decir, se da el caso (1) o el caso (3) y por lo tanto $1 \in M$.

(II) Supongamos que $b \in M$, es decir:

(1') $a = b$

o

(2') $b = a + n$

o

(3') $a = b + m$.

Para mostrar que $s(b) \in M$, debemos comparar a $s(b)$ con a. Para comenzar, en el caso (1') se tiene que $s(b) = s(a) = a + 1$ por lo que $a < s(b)$ y así $s(b) \in M$.

En el caso (2'), $b = a + n$ implica que $s(b) = s(a + n) = a + s(n)$ por lo que $a < s(b)$ y consecuentemente $s(b) \in M$.

En el caso (3'), $a = b + m$ por lo que $s(a) = s(b + m) = s(b) + m$. Si $m = 1$, de $a + 1 = s(b) + 1$ y la ley de cancelación para la suma se sigue que $a = s(b)$ por lo que $s(b) \in M$. Si $m \neq 1$, entonces $m = s(u)$ y así,

$$a + 1 = s(a) = s(b) + m = s(b) + s(u) = s(b) + u + 1$$

por lo que, usando la ley de cancelación para la suma, se sigue que $a = s(b) + u$ y consecuentemente $s(b) < a$, *i.e.*, $s(b) \in M$. Se sigue que $M = \mathbb{N}$, como se quería. □

EJERCICIO 1. Demuestre la *ley de cancelación para el producto en* $\mathbb{N}$: si $a, b, c \in \mathbb{N}$ y $ac = bc$, entonces $a = b$.

EJERCICIO 2. Demuestre la *compatibilidad del orden con las operaciones de* $\mathbb{N}$: si $a < b$ y $c \in \mathbb{N}$, entonces:

(1) $a + c < b + c$.

(2) $ac < bc$.

EJERCICIO 3. Usando el ejercicio anterior, demuestre que:

(1) Si $a, b, c, d \in \mathbb{N}$, $a < b$ y $c < d$, entonces $a + c < b + d$.

(2) Si $a, b, c, d \in \mathbb{N}$, $a < b$ y $c < d$, entonces $ac < bd$.

II.3 OTRAS FORMULACIONES DEL AXIOMA DE INDUCCIÓN

Recordando que un conjunto M lo podemos definir mediante una propiedad que caracterice a sus elementos, digamos

$$M = \{n \ : \ n \text{ satisface la propiedad } P(n)\},$$

en el caso que nos interesa cuando $M \subseteq \mathbb{N}$, la propiedad $P(n)$ es una propiedad de los números naturales, de tal forma que decir que $n \in M$ quiere decir que n satisface la propiedad P. Entonces, el axioma de inducción podríamos formularlo como sigue: *Si* $P(n)$ *es una propiedad de números naturales tal que:*

(I) *El número* 1 *satisface la propiedad* P.

(II) *Siempre que* $n \in \mathbb{N}$ *satisface la propiedad* P *se tiene que* $n + 1$ *también satisface la propiedad* P.

Entonces todo número natural satisface la propiedad P.

Esta formulación del axioma de inducción es útil para probar fórmulas en $\mathbb{N}$:

Ejemplo 1. Supongamos que queremos una fórmula para la suma de los primeros n números naturales:

$$1+2+3+\cdots+n.$$

Denotemos esta suma mediante $S(n) = 1+2+3+\cdots+n$ y observemos que escribiendo esta suma en orden inverso y sumando término a término queda:

$$\begin{array}{rcccccccccc} S(n) & = & 1 & + & 2 & + & \cdots & + & (n-1) & + & n \\ S(n) & = & n & + & (n-1) & + & \cdots & + & 2 & + & 1 \\ \hline 2S(n) & = & (n+1) & + & (n+1) & + & \cdots & + & (n+1) & + & (n+1) \end{array}$$

donde en el lado derecho hay n sumandos de la forma $(n+1)$ de tal forma que $2S(n) = n(n+1)$, *i.e.*,

$$S(n) = \frac{1}{2}n(n+1).$$

Por otra parte supongamos que alguien nos dice que se tiene la fórmula:

$$(*) \qquad 1+2+3+\cdots+n = \frac{1}{2}n(n+1)$$

sin haberla deducido como hicimos arriba y nos pide que mostremos que la fórmula $(*)$ es válida para todo $n \in \mathbb{N}$. Esto lo podemos hacer por inducción como sigue:

(I) La fórmula $(*)$ es cierta para $n = 1$ ya que el lado izquierdo es $= 1$, y el lado derecho es $= \frac{1}{2}1(1+1) = 1$.

(II) Supongamos ahora que $(*)$ es verdadera para el natural n. Mostraremos que es válida para $n+1$. En efecto,

$$\begin{aligned} 1+2+\cdots+n+(n+1) &= (1+2+3+\cdots+n)+(n+1) \\ &= \frac{1}{2}n(n+1)+(n+1) \quad \text{hipótesis de inducción} \\ &= (n+1)\left(\frac{1}{2}n+1\right) \quad \text{factorizando } (n+1) \\ &= (n+1)\left(\frac{n+2}{2}\right) \\ &= \frac{1}{2}(n+1)(n+2), \end{aligned}$$

que es precisamente la fórmula $(*)$ para el natural $n+1$. □

EJERCICIO 4. Si $a \in \mathbb{N}$ definimos las potencias a^n para cada $n \in \mathbb{N}$ como sigue:

$$a^1 := a,$$

y si a^n ya está definido, se define $a^{n+1} := a^n \cdot a$.

Demuestre que:

(I) $a^{m+n} = a^m a^n$, para cualesquiera $a, m, n \in \mathbb{N}$.

(II) $(a^m)^n = a^{mn}$, para cualesquiera $a, m, n \in \mathbb{N}$.

(III) $(ab)^n = a^n b^n$, para cualesquiera $a, b, n \in \mathbb{N}$.

(IV) $1^n = 1$, para cualquier $n \in \mathbb{N}$.

Ejemplo 2. Demuestre que $2^n > n \ \ \forall n \in \mathbb{N}$.

Demostración. Por inducción sobre n.

(I) Si $n = 1$, entonces $2^1 = 2 > 1$ ciertamente.

(II) Supongamos que $2^n > n$. Entonces

$$\begin{aligned} 2^{n+1} = 2^n \cdot 2 &> n \cdot 2 \qquad \text{por hipótesis de inducción} \\ &= n + n \geq n + 1, \end{aligned}$$

y así $2^{n+1} > n + 1$.

Ejemplo 3. Demuestre que $n^2 + n$ es par $\ \forall n \in \mathbb{N}$.

Demostración. Por inducción sobre n.

(I) Si $n = 1$, entonces $n^2 + n = 1^2 + 1 = 2$ que es par.

(II) Supongamos que $n^2 + n$ es par, es decir, que $n^2 + n = 2t$ para algún $t \in \mathbb{N}$. Entonces, cambiando n por $(n + 1)$ se tiene que:

$$(n+1)^2 + (n+1) = n^2 + 2n + 1 + (n+1) = (n^2 + n) + 2n + 2 = 2t + 2(n+1)$$

que es par; nótese que en la última igualdad se usó la hipótesis de inducción.

EJERCICIO 5. Usando inducción demuestre que:

(I) $1+4+9+\cdots+n^2=\dfrac{1}{6}n(n+1)(2n+1)$.

(II) $1+8+27+\cdots+n^3=\left(\dfrac{n(n+1)}{2}\right)^2$.

(III) $1+3+5+7+\cdots+(2n-1)=n^2$.

(IV) $1+2^n\leq 3^n$.

(V) $5+10+15+\cdots+5n=\dfrac{5n(n+1)}{2}$.

(VI) Si $n\geq 2$ y k son números naturales, entonces $(n-1)$ divide a (n^k-1).

Ejemplo 4 (Las torres de Hanoi). En un templo budista en Asia, los monjes tienen un juego que consiste en 3 torres (algo así como 3 postes) y 64 discos de tamaño diferente, ordenados de arriba hacia abajo con el mayor disco abajo y el menor arriba, de tal forma que encima de cualquier disco dado no hay un disco mayor que el disco dado. Los discos se hallan acomodados en, digamos, la torre A, y el problema es trasladar todos los discos a la torre C (usando a la torre B como intermediaria) de acuerdo con las reglas siguientes: (I) sólo se puede mover un disco a la vez, (II) nunca se puede poner un disco de tamaño mayor sobre un disco de tamaño menor. Por supuesto que, si no existiera la torre B, el problema no tendría solución. Para hacer el problema más interesante, podemos pensar que se tienen n discos y que queremos hallar el *menor* número de movidas para llevar los discos de A a C.

Para resolver el problema, comencemos numerando los discos llamando 1 al disco menor (el de arriba) y así sucesivamente hasta llegar al disco n (el disco de abajo). Llamemos $T(n)$ al número mínimo de movidas necesarias para llevar los n discos de A a C. Para comenzar, si el número de discos es $n=1$, el problema se resuelve trivialmente y $T(1)=1$.

Para el caso general, consideremos los $n-1$ discos superiores (es decir, no consideramos el disco grande de abajo). Nuestra hipótesis de inducción será que estos $n-1$ discos se pueden llevar a la torre B (usando C como intermediaria) en $T(n-1)$ movidas, de tal forma que ya liberamos al disco grande n, el cual puede ser trasladado en una movida a la torre C. Ahora tenemos el disco grande en el lugar requerido, pero tenemos los otros $n-1$ discos en la torre B, los cuales podemos trasladar a la torre C, encima

del disco grande ya colocado, usando ahora a la torre A como intermediaria. Esto se hace por hipótesis de inducción en $T(n-1)$ movidas. Así, ya llevamos todos los discos, en el menor número de movidas, a la torre C, y el número $T(n)$ de movidas requeridas fue:

$$(*) \qquad T(n) = T(n-1) + 1 + T(n-1) = 2T(n-1) + 1.$$

Algunas observaciones acerca de este resultado: notamos de inmediato que ésta no es una fórmula en la cual podemos substituir $n = 64$ para resolver directamente el problema de los monjes. De hecho, notamos que para calcular $T(64)$ debemos calcular primero $T(63)$ ya que $T(64) = 2T(63) + 1$. Similarmente, para calcular $T(63)$ debemos calcular primero $T(62)$, y así sucesivamente. Decimos que $(*)$ es una *fórmula recursiva*. Cuando un resultado viene expresado en una fórmula recursiva como la anterior, es deseable obtener una *fórmula cerrada*, *i.e.*, que sólo dependiera de n para poder calcular directamente el resultado deseado sin necesidad de calcular todos los términos anteriores. En ocasiones obtener tal fórmula cerrada no es una empresa fácil, sin embargo, en el caso en consideración, podemos proceder como sigue: sabemos que $T(1) = 1$, por lo que $T(2) = 2T(1) + 1 = 2 + 1 = 3$. Se sigue que $T(3) = 2T(2) + 1 = 6 + 1 = 7$, y sucesivamente $T(4) = 14 + 1 = 15$, $T(5) = 30 + 1 = 31$, $T(6) = 63$, $T(7) = 127$, $T(8) = 255$, etc. Si observamos estos números, parece razonable suponer que

$$(\dagger) \qquad T(n) = 2^n - 1.$$

Probaremos $(\dagger)$, por inducción sobre n, usando la fórmula recursiva $(*)$. Para $n = 1$, se tiene que $2^1 - 1 = 1 = T(1)$, como se quería. Supongamos el resultado válido para $n - 1$, i.e. que $T(n-1) = 2^{n-1} - 1$. Entonces, para el entero n, se tiene que

$$\begin{aligned} T(n) &= 2T(n-1) + 1 && \text{por la fórmula } (*) \\ &= 2(2^{n-1} - 1) + 1 && \text{por hipótesis de inducción} \\ &= 2^n - 2 + 1 \\ &= 2^n - 1, \end{aligned}$$

que es la fórmula deseada.

EJERCICIO 6. Defina la sucesión siguiente: $s_0 = 1 = s_1$ y, si $n \geq 2$, $s_n := s_{n-1} + s_{n-2}$.

- Calcule los primeros 10 términos de la sucesión.
- Usando inducción, demuestre que

$$s_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} \qquad \text{para } n \geq 2$$

donde α y β son las raíces de la ecuación cuadrática $x^2 - x - 1 = 0$. *Sugerencia*: demuestre primero que $\alpha = 1 + \dfrac{1}{\alpha}$ y similarmente para β. De aquí se sigue que $\alpha^{n+2} = \alpha^{n+1} + \alpha^n$ y similarmente para β.

- La sucesión anterior se conoce como la *sucesión de Fibonacci*. Investigue quién fue Fibonacci.

EJERCICIO 7. Sea p_n el n-ésimo entero primo. Por ejemplo, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, etcétera.

- Calcule p_n para $n \leq 100$.
- Demuestre que $p_{n+1} \leq p_1 \cdots p_n + 1$.
- Usando inducción y el inciso anterior, demuestre que $p_n \leq 2^{2^{n-1}}$.

EJERCICIO 8 (La moneda falsa). Suponga que se tienen 3^n monedas y se sabe que una de ellas es falsa y pesa menos que las otras. Suponga también que se tiene una báscula con dos platos sin graduación ni pesas para la báscula, de tal manera que la única forma de pesar las monedas es poner algunas en un plato y otras monedas en el otro plato y comparar si los platos quedan o no balanceados. Con este procedimiento usted tiene que encontrar la moneda falsa. Usando inducción demuestre que n pesadas bastan para encontrar la moneda falsa. Explique.

EJERCICIO 9. Suponga que se tiene un conjunto finito de canicas cualquiera y se quiere probar que no importa cuál sea este conjunto, todas las canicas son de un solo color (!!!!!). La demostración de esta afirmación es por inducción sobre el número n de canicas del conjunto dado:

(I) Si $n = 1$, no hay nada que probar.

(II) Supongamos que el resultado es válido para conjuntos con menos de n canicas y supongamos que tenemos un conjunto con n canicas y queremos probar que todas éstas son del mismo color. Enumeremos estas n canicas como: $c_1, c_2, \ldots, c_n$. Si quitamos la canica c_n queda el conjunto $c_1, \ldots, c_{n-1}$ con $(n-1) < n$ canicas y así, por hipótesis de inducción, todas las canicas $c_1, \ldots, c_{n-1}$ son del mismo color. Similarmente, si quitamos la canica c_1, el conjunto $\{c_2, \ldots, c_n\}$ tiene $(n-1) < n$ canicas y por hipótesis de inducción todas éstas son del mismo color. Notamos ahora que los conjuntos $\{c_1, c_2, \ldots, c_{n-1}\}$ y $\{c_2, \ldots, c_n\}$ tienen la canica c_2 en común y por lo tanto todas las canicas $c_1, c_2, \ldots, c_n$ son del mismo color, como se quería demostrar. ¿Qué está mal con el argumento anterior?

EJERCICIO 10. Considere la sucesión de enteros definida recursivamente por $s_0 = 4$ y si $n \geq 1$, $s_n = s_{n-1}^2 - 2$.

(I) Calcule los primeros 5 términos de la sucesión.

(II) Sean $\omega = 2 + \sqrt{3}$ y $\overline{\omega} = 2 - \sqrt{3}$. Usando inducción sobre n, demuestre que

$$s_n = \omega^{2^n} + \overline{\omega}^{2^n}$$

II.4 El principio del buen orden

Usando el orden $<$ en $\mathbb{N}$ introducido en la sección § II.2, podemos definir una relación de orden parcial $\leq$ en $\mathbb{N}$ de la forma natural: si $a, b \in \mathbb{N}$ se define $a \leq b$ (se lee: a es *menor o igual que* b) si $a = b$ o $a < b$.

EJERCICIO 11. Demuestre que la relación $\leq$ en $\mathbb{N}$ es reflexiva, antisimétrica y transitiva, *i.e.,* es un *orden parcial* (véase la parte final de la sección § I.3 para una discusión de la noción de *orden parcial* en un conjunto arbitrario).

En ocasiones también usaremos el orden parcial $a \geq b$ (se lee: a es mayor o igual que b) definido mediante $a \geq b \Leftrightarrow b \leq a$.

En § II.2 probamos que el orden $<$ en $\mathbb{N}$ satisface la propiedad de tricotomía (II.16). Ésta es una propiedad importante para cualquier orden parcial en un conjunto y cuando éste la satisfaga diremos que el orden es un *orden total o lineal.* En general, si $(A, \preceq)$ es un conjunto parcialmente

ordenado, se define $a \prec b \Leftrightarrow a \preceq b$ pero $a \neq b$, y se dice que el orden $\preceq$ es un *orden total o lineal* si se satisface la *ley de tricotomía* : para cualesquiera $a, b \in A$ se cumple exactamente uno de los tres casos siguientes:

(I) $a \prec b$

(II) $a = b$

(III) $b \prec a$

y se dice que el conjunto A es un *conjunto totalmente ordenado.*

Ejemplo 5. Por (II.16), el orden $\leq$ en $\mathbb{N}$ es un orden total.

Ejemplo 6. El orden parcial $a \preceq b$ dado por $a|b$ en $\mathbb{N}$ no es un orden total, ya que dados $a, b \in \mathbb{N}$ no siempre se tiene que $a|b$ o $a = b$ o $b|a$; un ejemplo sería $a = 2$ y $b = 3$.

Aun cuando el orden $a \leq b$ nos puede parecer natural, ya que nos parece obvio que los números naturales vayan ordenados en la lista:

$$1, 2, 3, 4, 5, \ldots,$$

existen otras maneras de ordenar a $\mathbb{N}$, como se muestra en los ejemplos siguientes:

Ejemplo 7. En $\mathbb{N}$ se define la relación $\preceq$ mediante

$$m \preceq n \Leftrightarrow \begin{cases} m, n \text{ son pares} & \text{y} \quad m \leq n \\ m, n \text{ son impares} & \text{y} \quad m \leq n \\ m \text{ es par} & \text{y} \quad n \text{ es impar.} \end{cases}$$

Éste es un orden total en $\mathbb{N}$ que lista a los naturales como:

$$2, 4, 6, 8, \ldots, 1, 3, 5, 7, \ldots$$

EJERCICIO 12. En $\mathbb{N}$ se define la relación $\preceq$ mediante

$$m \preceq n \Leftrightarrow \begin{cases} m, n \text{ son pares} & \text{y} \quad m \leq n \\ m, n \text{ son impares} & \text{y} \quad m \leq n. \end{cases}$$

Muestre que éste es un orden parcial que no es total.

EJERCICIO 13. Otro orden total $\preceq$ en $\mathbb{N}$ está dado por:

$$m \preceq n \Leftrightarrow \begin{cases} m, n \text{ son pares} & \text{y} \quad m \geq n \\ m, n \text{ son impares} & \text{y} \quad m \leq n \\ m \text{ es par} & \text{y} \quad n \text{ es impar.} \end{cases}$$

Con este orden los elementos de $\mathbb{N}$ se ven como sigue:

$$\ldots, 6, 4, 2, 1, 3, 5, \ldots$$

Nótese que una diferencia esencial entre este orden total en $\mathbb{N}$ y los dados por el orden "natural" $m \leq n$ del ejemplo 5 y el orden del ejemplo 7 es que en el orden del ejercicio 13 no hay un primer elemento:

DEFINICIÓN II.17. Si $\preceq$ es un orden total en $\mathbb{N}$ y $M \subseteq \mathbb{N}$, un elemento $c \in M$ se dice que es un *primer elemento o elemento menor* de M si para todo $x \in M$ se tiene que $c \preceq x$.

EJERCICIO 14. Si $\preceq$ es un orden total en $\mathbb{N}$ y $M \subseteq \mathbb{N}$ tiene un primer elemento, demuestre que éste es único.

En general, puede suceder que algún subconjunto M no tenga un primer elemento, por ejemplo si $M = \mathbb{N}$ con el orden dado por el ejercicio 13.

DEFINICIÓN II.18. Si $\preceq$ es un orden total en $\mathbb{N}$, diremos que éste es un *buen orden* o que satisface el *principio de buen orden*, si todo subconjunto no vacío $M \subseteq \mathbb{N}$ tiene un primer elemento, *i.e.,* existe un $n_0 \in M$ tal que $n_0 \preceq n$ para todo $n \in M$.

Así, el orden del ejercicio 13 no es un buen orden. El orden del ejemplo 7 sí es un buen orden y el orden "natural" $\leq$ en $\mathbb{N}$ del ejemplo 5 también es un buen orden, como probaremos en el teorema II.19, más adelante. De hecho, veremos que, con el orden $\leq$ esencialmente definido usando la suma de $\mathbb{N}$, que a su vez usa el principio de inducción para su definición y para probar sus propiedades esenciales, $(\mathbb{N}, \leq)$ satisface el principio del buen orden.

Más aún, veremos a continuación que, bajo las condiciones apropiadas, el principio del buen orden en $(\mathbb{N} \preceq)$ implica el principio de inducción. Estas condiciones son aquellas que garantizan que el orden $\preceq$ se comporta como el orden $\leq$ (definido usando la suma en $\mathbb{N}$, *i.e.,* usando el principio de inducción), es decir, queremos que el conjunto $\mathbb{N}$ satisfaga los primeros

cuatro axiomas de Peano y que además el buen orden $\preceq$ sea *compatible* con la función sucesor $s : \mathbb{N} \to \mathbb{N}$, *i.e.*, que satisfaga que

$$m \prec s(m) \quad \forall m \in \mathbb{N}$$

y que $1 \in \mathbb{N}$ sea el único elemento que no tenga predecesor, *i.e.*, que se tenga la conclusión del lema (II.2). Esto es importante porque en el orden del ejemplo 7, el $2 \in \mathbb{N}$ y el $1 \in \mathbb{N}$ no tienen predecesores.

Resumiendo, el teorema siguiente nos dice que el principio de inducción (PI) es equivalente al principio del buen orden (PBO) bajo las condiciones apropiadas, y la importancia del teorema II.19 radica en que, en ocasiones, el PBO es más fácil de usar que el principio de inducción, como tendremos oportunidad de ver en el capítulo siguiente.

TEOREMA II.19. (1) *El principio de inducción* (PI) *en* $\mathbb{N}$ *implica el principio de buen orden* (PBO), *es decir, con el orden "natural"* $\leq$, *el conjunto* $\mathbb{N}$ *satisface el* PBO.

(2) *Recíprocamente, si* $\mathbb{N}$ *satisface los primeros cuatro axiomas de Peano y además tiene un buen orden* $\preceq$ *que es compatible con la función sucesor* $s : \mathbb{N} \to \mathbb{N}$, *i.e., que satisface que*

(I) $m \prec s(m) \quad \forall m \in \mathbb{N}$

y

(II) $s : \mathbb{N} \to \mathbb{N} - \{1\}$ *es suprayectiva,*

entonces $\mathbb{N}$ *satisface el principio de inducción.*

Demostración. Mostraremos que el PI implica el PBO. Supongamos que existe un subconjunto $M \subseteq \mathbb{N}$ que no tiene elemento menor. Mostraremos que $M = \emptyset$. En efecto, sea

$$M' := \{n \in \mathbb{N} \ : \ \forall\, x \in M \text{ se tiene que } x \geq n\}.$$

Probaremos, por inducción, que $M' = \mathbb{N}$. En efecto,

(I) $1 \in M'$ ya que para todo $x \in \mathbb{N}$ se tiene que $x \geq 1$, en particular para todo $x \in M$, $x \geq 1$.

(II) Supongamos que $n \in M'$, *i.e.*, que $\forall\, x \in M$ se tiene que $x \geq n$. Entonces, para comenzar n no puede estar en M ya que si esto sucediera entonces $n \in M$ satisface que $x \geq n\ \forall\, x \in M$ y por lo tanto $n \in M$ sería un elemento

menor de M, en contradicción con la hipótesis sobre M. Se sigue que $n \notin M$ y como $\forall\, x \in M$ se tiene que $x \geq n$ entonces se debe tener que $x > n$ para todo $x \in M$, es decir, $\forall\ x \in M$ se tiene que $x \geq n+1$ y por lo tanto $n+1 \in M'$.

Por el principio de inducción se sigue que $M' = \mathbb{N}$ y por lo tanto $M = \emptyset$.

Mostraremos que el PBO implica el PI. Sea $M \subseteq \mathbb{N}$ un subconjunto que satisface: $1 \in M$ y siempre que $n \in M$ se tiene que $s(n) \in M$. Probaremos que $M = \mathbb{N}$. En efecto, si $M \neq \mathbb{N}$ entonces $M^c = \mathbb{N} - M \neq \emptyset$ y así, por el PBO el conjunto M^c tiene un elemento menor $n_0 \in M^c$. Ahora, como $1 \notin M^c$ entonces $n_0 \neq 1$ y así, por (II), $n_0 = s(m_0)$ con $m_0 \in \mathbb{N}$. Por (I) se sigue que $m_0 \prec n_0$ y así $m_0 \notin M^c$ ya que n_0 es el menor elemento de M^c, por lo que $m_0 \in M$; pero este elemento satisface que $s(m_0) = n_0 \notin M$, lo cual es una contradicción con una de las hipótesis que satisface M. Se debe entonces tener que $M^c = \emptyset$ y así $M = \mathbb{N}$. □

EJERCICIO 15. Usando el principio de buen orden, demuestre que no existe un número natural entre 1 y 2.

EJERCICIO 16. En general, demuestre que no existe un número natural entre n y $n+1$, para todo $n \in \mathbb{N}$.

II.5 CONTAR

Al inicio de este capítulo recordamos que los números naturales aparecen en forma *natural* al contar los elementos de algunos conjuntos. En esta sección formalizaremos lo anterior. Dados dos conjuntos A y B, diremos que A tiene el *mismo cardinal* que B si existe una función biyectiva $f : A \to B$. Como la inversa de una función biyectiva también es biyectiva, si A tiene el mismo cardinal que B entonces B tiene el mismo cardinal que A, y como la composición de funciones biyectivas es biyectiva, entonces es claro que la relación: *tienen el mismo cardinal*, es una relación de equivalencia entre los (sub)conjuntos de un conjunto X dado.

Si $n \in \mathbb{N}$, se define el *intervalo de naturales* $\mathbb{I}_n := \{1, 2, \ldots, n\} \subsetneq \mathbb{N}$ y para $n = 0$ se define $\mathbb{I}_0 = \emptyset$ (el conjunto vacío). Un conjunto A se dice que es *finito* si existe una biyección $\phi : A \to \mathbb{I}_n$ para algún intervalo $\mathbb{I}_n$. Un *conjunto infinito* es un conjunto que no es finito.

La idea de contar los elementos de un conjunto finito A es establecer una biyección entre A y algún intervalo $\mathbb{I}_n$ y uno dice entonces que A tiene n elementos. Surge entonces la pregunta de que si no pudiera suceder que se tienen biyecciones $A \to \mathbb{I}_m$ y $A \to \mathbb{I}_n$ con $m \neq n$. Que esto no sucede es consecuencia de los resultados siguientes que, al principio, pueden parecer obvios a la lectora o lector:

TEOREMA II.20. *Sean $m, n \in \mathbb{N} \cup \{0\}$. Si $m \neq n$, entonces no existe una biyección $\phi : \mathbb{I}_m \to \mathbb{I}_n$.*

NOTA. Por definición diremos que $0 < k$ para todo $k \in \mathbb{N}$.

Demostración. Como $m \neq n$, entonces $m < n$ o $n < m$ y, para comenzar, observe que basta probar el teorema en el primer caso, ya que si $n < m$ y si existiera una biyección $f : \mathbb{I}_m \to \mathbb{I}_n$ entonces su inversa $f^{-1} : \mathbb{I}_n \to \mathbb{I}_m$ sería una biyección, en contradicción con el primer caso. Probaremos ahora el primer caso por inducción sobre m, comenzando con $m = 0$:

(I) Si $m = 0$ y $n > 0$, claramente no hay ninguna biyección del conjunto vacío $\mathbb{I}_0 = \emptyset$ al conjunto no vacío $\mathbb{I}_n$ $(n > 0)$.

(II) Supongamos que la afirmación es válida para m y todo $n > m$. Para $m + 1$, supongamos que existe una biyección $f : \mathbb{I}_{m+1} \to \mathbb{I}_n$ para algún $n > m+1$. Escribamos $\mathbb{I}_{m+1} = \mathbb{I}_m \cup \{m+1\}$ y pongamos $f(m+1) = k \in \mathbb{I}_n$. Sea $\phi : \mathbb{I}_n \to \mathbb{I}_n$ la función que intercambia k y n y deja fijos a los otros elementos, es decir:

$$\phi(j) = \begin{cases} k & \text{si } j = n \\ n & \text{si } j = k \\ j & \text{si } j \neq k, n \end{cases}$$

y observemos que $(\phi \circ \phi)(k) = \phi(n) = k$ y $(\phi \circ \phi)(n) = n$ por lo que $\phi \circ \phi = \mathrm{id}_{\mathbb{I}_n}$, *i.e.,* ϕ es una biyección con inversa ella misma.

Entonces, la composición $g = f \circ \phi : \mathbb{I}_{m+1} \xrightarrow{f} \mathbb{I}_n \xrightarrow{\phi} \mathbb{I}_n$ es biyectiva, ya que f lo es por la suposición inicial y ϕ lo es por lo observado arriba. Nótese que $g(m+1) = n$. Entonces, restringiendo el dominio de g al subconjunto $\mathbb{I}_m \subseteq \mathbb{I}_{m+1}$ y restringiendo el codominio de g a $\mathbb{I}_{n-1} = \mathbb{I}_n - \{n\}$, se obtiene la función $\widetilde{g} : \mathbb{I}_m \to \mathbb{I}_{n-1}$ dada por $\widetilde{g}(i) = g(i)$. Es claro entonces que $\widetilde{g} : \mathbb{I}_m \to \mathbb{I}_{n-1}$ es biyectiva, pero como $m < n - 1$ (ya que $m + 1 < n$), esto contradice la hipótesis de inducción. Se sigue que no puede existir una biyección $f : \mathbb{I}_{m+1} \to \mathbb{I}_n$ para todo $n > m + 1$. □

COROLARIO II.21. *Si A es un conjunto finito, entonces existe un único $\mathbb{I}_n$ tal que se tiene una biyección $f : A \to \mathbb{I}_n$.*

Demostración. Si se tienen biyecciones $f : A \to \mathbb{I}_n$ y $g : A \to \mathbb{I}_m$, entonces $f \circ g^{-1} : \mathbb{I}_m \to \mathbb{I}_n$ también es biyectiva y así por el teorema anterior $m = n$. □

Gracias a este resultado, a cada conjunto finito A le podemos asociar un único número $n \in \mathbb{N} \cup \{0\}$ y diremos que A tiene n elementos. En otras palabras, este corolario nos permite contar conjuntos finitos. Se suele usar la notación $n = |A| = \#(A)$. Vale la pena repetirlo: contar un conjunto finito A es establecer una biyección

$$f : A \to \mathbb{I}_n$$

y el conjunto $\mathbb{I}_n$ correspondiente es único.

LEMA II.22. *Para todo $n \in \mathbb{N} \cup \{0\}$, cualquier función inyectiva $f : \mathbb{I}_n \to \mathbb{I}_n$ es suprayectiva.*

Demostración. Por inducción sobre n:

(I) Si $n = 0$, entonces $\mathbb{I}_0 = \emptyset$ y no hay nada que probar.

(II) Supongamos que la afirmación es válida para n y sea $f : \mathbb{I}_{n+1} \to \mathbb{I}_{n+1}$ una función inyectiva. Sea $k = f(n+1)$ y consideremos la función biyectiva $\phi : \mathbb{I}_{n+1} \to \mathbb{I}_{n+1}$ que intercambia k y $n+1$ como en la demostración del teorema anterior. Entonces, la composición $g = \phi \circ f$ es tal que $g(n+1) = n+1$ por lo que la restricción $\widetilde{g}$ de g a $\mathbb{I}_n$, *i.e.*, $\widetilde{g} : \mathbb{I}_n \to \mathbb{I}_n$ es inyectiva. Por hipótesis de inducción se sigue que $\widetilde{g}$ es suprayectiva y por lo tanto es biyectiva; se sigue que g también es biyectiva y como $\phi \circ f = g$ con ϕ biyectiva, se sigue que $f = \phi^{-1} \circ g$ con ϕ^{-1} y g biyectivas por lo que f también es biyectiva, como se quería. □

EJERCICIO 17. En forma similar, demuestre que para todo $n \in \mathbb{N} \cup \{0\}$, cualquier función suprayectiva $f : \mathbb{I}_n \to \mathbb{I}_n$ es inyectiva.

PROPOSICIÓN II.23. *Si A es un conjunto finito, entonces una función $f : A \to A$ es suprayectiva si y sólo si es inyectiva.*

Demostración. Como A es finito, entonces existe una biyección $\phi : \mathbb{I}_n \to A$. Consideremos entonces la composición

$$g : \mathbb{I}_n \xrightarrow{\phi} A \xrightarrow{f} A \xrightarrow{\phi^{-1}} \mathbb{I}_n$$

y observemos que f suprayectiva implica que la composición g es suprayectiva y similarmente f inyectiva implica g inyectiva. Así, basta probar la proposición para $A = \mathbb{I}_n$.

Observamos ahora que el lema previo dice que toda función $g : \mathbb{I}_n \to \mathbb{I}_n$ inyectiva es suprayectiva. Recíprocamente, el ejercicio anterior nos dice que toda función $g : \mathbb{I}_n \to \mathbb{I}_n$ suprayectiva es inyectiva. □

Ejercicio 18. Demuestre que existe una inyección $\mathbb{I}_m \to \mathbb{I}_n$ si y sólo si $m \leq n$.

Observación. Algunas veces, a la afirmación del ejercicio anterior se le suele llamar el *principio del palomar*, debido a la interpretación siguiente: pensando a los elementos de $\mathbb{I}_m$ como palomas y a los elementos de $\mathbb{I}_n$ como las casillas de un palomar, una función $f : \mathbb{I}_m \to \mathbb{I}_n$ asigna palomas a casillas del palomar. Así, cuando $m > n$ el ejercicio previo nos dice que *ninguna* función $f : \mathbb{I}_m \to \mathbb{I}_n$ puede ser inyectiva, *i.e.*, para cualquier asignación de palomas en el palomar, en alguna casilla hay más de una paloma. En este lenguaje, el principio del palomar se enuncia como sigue: *si hay más palomas que casillas en un palomar, entonces alguna casilla contiene más de una paloma.*

Ejercicio 19. Demuestre que existe una suprayección $\mathbb{I}_m \to \mathbb{I}_n$ si y sólo si $m \geq n$.

II.6 Principios elementales de conteo

En la sección anterior formalizamos la noción de *contar* un conjunto finito A, estableciendo una biyección entre este conjunto A y un intervalo $\mathbb{I}_n$ de $\mathbb{N}$. De esta manera, la biyección $f : A \to \mathbb{I}_n$ decimos que *enumera* los elementos del conjunto A, en cierta forma poniéndolos en una *lista*. Ahora bien, en ocasiones puede suceder que no tengamos una forma inmediata de enlistar los elementos del conjunto A y éste sólo viene definido por unas propiedades que cumplen sus elementos. En esta sección desarrollamos ciertos métodos que nos permitirán contar los elementos del conjunto A, a los que se llama *principios elementales de conteo* que, de alguna manera, no necesitan dar una biyección explícita para contar los elementos de un conjunto finito dado. Los resultados preliminares para establecer estos principios de conteo usan, sin embargo, biyecciones explícitas, lo cual no debe parecernos extraño:

PROPOSICIÓN II.24 (Principio básico de la suma). *Si A y B son conjuntos finitos disjuntos (i.e., $A \cap B = \emptyset$), entonces*

$$|A \cup B| = |A| + |B|.$$

Demostración. Como A y B son finitos, existen biyecciones $f : A \to \mathbb{I}_m$ y $g : B \to \mathbb{I}_n$, es decir, $|A| = m$ y $|B| = n$. Queremos probar que $|A \cup B| = m + n$, es decir, queremos una biyección

$$h : A \cup B \to \mathbb{I}_{m+n}.$$

Ahora, si observamos que

$$\mathbb{I}_{m+n} = \mathbb{I}_m \cup \{m+1, m+2, \ldots, m+n\},$$

la función h que queremos la definimos como sigue:

$$h(x) := \begin{cases} f(x) & \text{si } x \in A \\ m + g(x) & \text{si } x \in B. \end{cases}$$

Para comenzar, es claro que h es una función ya que si $x \in A \cup B$, entonces $x \in A$ o $x \in B$ (pero x no puede estar en ambos conjuntos porque $A \cap B = \emptyset$). Si $x \in A$, entonces $h(x) = f(x) \in \mathbb{I}_m \subseteq \mathbb{I}_{m+n}$. Si $x \in B$, entonces $g(x) \in \mathbb{I}_n$ por lo que $1 \leq g(x) \leq n$ y consecuentemente $m+1 \leq m+g(x) \leq m+n$, *i.e.*, $h(x) = m + g(x) \in \{m+1, \ldots, m+n\} \subseteq \mathbb{I}_{m+n}$. Dejamos como un ejercicio el mostrar que h es biyectiva. □

EJERCICIO 20. Demuestre que h es biyectiva.

EJERCICIO 21. Si $A \subseteq B$ son conjuntos finitos, demuestre que $|A| \leq |B|$. *Sugerencia*: $B = A \cup (B - A)$.

EJERCICIO 22. Si A, B son conjuntos finitos y $f : A \to B$ es una función inyectiva, demuestre que $|A| = |f(A)|$. Concluya que $|A| \leq |B|$.

EJERCICIO 23. Si A, B son conjuntos finitos y $f : A \to B$ es una función suprayectiva, demuestre que $|A| \geq |B|$.

Una generalización directa de la proposición anterior es:

COROLARIO II.25 (Principio de la suma). *Si $A_1, \ldots, A_k$ son conjuntos finitos disjuntos por pares (i.e., $A_i \cap A_j = \emptyset$ si $i \neq j$), entonces*

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.$$

Demostración. Se sigue de la proposición anterior por inducción sobre k, comenzando con $k = 2$. □

Otra consecuencia es el *principio del palomar* que, recordamos, nos dice que *si hay más palomas que casillas en un palomar, entonces alguna casilla tiene más de una paloma.* Dicho en otras palabras: *si se distribuyen m objetos en n cajas, con $m > n$, entonces al menos una caja tiene más de un objeto.* Para formalizar este enunciado, pensemos a los m objetos como elementos de un conjunto A de tal forma que $|A| = m$, y las n cajas conteniendo objetos de A como subconjuntos $A_i \subseteq A$ para $1 \leq i \leq n$ que además satisfacen que son disjuntos por pares y $A = A_1 \cup \cdots \cup A_n$. Así, el principio del palomar formalmente lo podemos enunciar como sigue:

COROLARIO II.26 (Principio del palomar). *Supongamos que $|A| = m$ y se tienen n subconjuntos $A_i \subseteq A$, $1 \leq i \leq n$, disjuntos por pares, tales que $A = A_1 \cup \cdots \cup A_n$. Si $m > n$, entonces algún A_i tiene cardinalidad $|A_i| > 1$.*

Demostración. Supongamos que el resultado no es cierto, *i.e.*, supongamos que $|A_i| \leq 1$ para toda i. Entonces,

$$\begin{aligned} m = |A| &= |A_1 \cup \cdots \cup A_n| \\ &= |A_1| + \cdots + |A_n| && \text{por el corolario anterior} \\ &\leq \overbrace{1 + \cdots + 1}^{n} && \text{porque } |A_i| \leq 1 \text{ para toda } i \\ &= n, \end{aligned}$$

i.e., $m \leq n$, en contradicción con la hipótesis de que $m > n$. □

Este corolario se puede generalizar como sigue:

EJERCICIO 24. Si se distribuyen m objetos en n cajas, con $m > nr$ para algún $r \geq 1$, entonces al menos una caja tiene más de r objetos.

EJERCICIO 25. El principio básico de donde obtuvimos los corolarios anteriores requería que A y B fueran disjuntos. Usando este principio básico, demuestre que, en general,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

EJERCICIO 26. Considere ahora tres conjuntos finitos A, B, C no necesariamente disjuntos por pares. Obtenga una fórmula para la cardinalidad de $A \cup B \cup C$ que generalice, para $k = 3$, el primer corolario del principio básico de la suma y la fórmula del ejercicio anterior.

Dados conjuntos finitos A y B, además de las operaciones de *unión* e *intersección* para obtener nuevos conjuntos, tenemos la operación producto cartesiano

$$A \times B = \{(a, b) \ : \ a \in A, b \in B\}.$$

Como los conjuntos A y B son finitos, digamos

$$A = \{x_1, \ldots, x_m\} \qquad B = \{y_1, \ldots, y_n\},$$

podemos representar subconjuntos del producto cartesiano $A \times B$ por medio de una tabla:

	y_1	y_2	$\cdots$	y_n
x_1	•		•	
x_2		•		
x_3				•
$\vdots$				
x_m	•			

donde los puntos • indican el par ordenado (x_i, y_j) en el lugar correspondiente.

Las técnicas de conteo anteriores las usaremos ahora para contar los elementos del producto cartesiano $A \times B$:

PROPOSICIÓN II.27 (Principio básico del producto). *Si A y B son conjuntos finitos, entonces*

$$|A \times B| = |A||B|.$$

Demostración. Supongamos que $A = \{a_1, \ldots, a_m\}$ de tal forma que $|A| = m$. Observemos primero que todas las columnas $\{a_i\} \times B$, variando $a_i \in A$, tienen la misma cardinalidad que B; de hecho, existe una biyección

$$\rho_i : \{a_i\} \times B \to B$$

dada por la función $\rho_i(a_i, b) := b$. Se sigue que $|\{a_i\} \times B| = |B|$ para cada $a_i \in A$.

Observemos después que las columnas $\{a_i\} \times B \subseteq A \times B$ forman una partición de $A \times B$, en particular estas columnas son disjuntas por pares y su unión es todo $A \times B$. Por el principio de la suma se sigue que

$$|A \times B| = \sum_{i=1}^{m} |\{a_i\} \times B| = \sum_{i=1}^{m} |B| = m|B| = |A||B|. \qquad \square$$

EJERCICIO 27. Demuestre que la función $\rho_i : \{a_i\} \times B \to B$ dada por la función $\rho_i(a_i, b) := b$ es una biyección.

EJERCICIO 28. Demuestre que los subconjuntos $\{a_i\} \times B$ forman una partición de $A \times B$.

Una generalización directa de la proposición anterior es:

COROLARIO II.28 (Principio del producto). *Si $A_1, \ldots, A_k$ son conjuntos finitos, entonces*

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1||A_2| \cdots |A_k|.$$

Demostración. Se sigue de la proposición anterior por inducción sobre k, comenzando con $k = 2$. $\square$

Aplicaremos este corolario para determinar el *número de funciones* que puede haber entre un conjunto A y un conjunto B, ambos finitos. Supongamos que $A = \{a_1, a_2, \ldots, a_m\}$ de tal forma que $|A| = m$. Pongamos $n = |B|$. Una función $f : A \to B$ está determinada por sus valores $f(a_1), f(a_2), \ldots, f(a_m)$ en B. Considerando el orden dado por los subíndices de los a_j, podemos pensar al conjunto de valores de f como un m-ada ordenada en $B^m := \overbrace{B \times \cdots \times B}^{m}$. Así, denotando con

$$B^A := \{f : A \to B \ : \ f \text{ es una función}\},$$

podemos definir una función

$$\psi : B^A \to B^m$$

mediante $f \mapsto (f(a_1), f(a_2), \ldots, f(a_m))$. Mostraremos que ψ es biyectiva. Claramente es suprayectiva, ya que si $(b_1, \ldots, b_m) \in B^m$, definiendo la función $f \in B^A$ mediante $f(a_i) = b_i$, para $1 \leq i \leq m$, se tiene que $\psi(f) = (f(a_1), \ldots, f(a_m)) = (b_1, \ldots, b_m)$. Que ψ es inyectiva es porque si $\psi(f) = \psi(g)$, entonces

$$(f(a_1), \ldots, f(a_m)) = (g(a_1), \ldots, g(a_m))$$

por lo que $f(a_i) = g(a_i)$ para toda $a_i \in A$. Se sigue que $f = g$.

PROPOSICIÓN II.29. *Sean A y B conjuntos finitos. Entonces,*

$$\left|B^A\right| = |B|^{|A|}.$$

Demostración. Si $|A| = m$, hemos mostrado arriba que existe una biyección

$$\psi : B^A \to B^m$$

y por el corolario anterior se tiene que $|B^m| = |B|^m = |B|^{|A|}$, por lo que $\left|B^A\right| = |B|^{|A|}$. □

Ejemplo 8. Usando el resultado anterior, contaremos el *número de subconjuntos* que tiene un conjunto finito A. Para esto, pongamos $|A| = m$. Para cada subconjunto $M \subseteq A$, definimos su *función característica* $f_M : A \to \{0, 1\}$ mediante

$$f_M(x) := \begin{cases} 1 & \text{si } x \in M \\ 0 & \text{si } x \notin M. \end{cases}$$

Observe que la función f_M detecta exactamente los elementos de A que pertenecen al subconjunto M y en este sentido *caracteriza* al subconjunto M. Recíprocamente, cada función $f : A \to \{0, 1\}$ determina el subconjunto $M = \{x \in A \ : \ f(x) = 1\} \subseteq A$. Hemos así mostrado que existe una biyección entre el conjunto de subconjuntos de A y el conjunto de funciones $\{0, 1\}^A$. Se sigue que el número de subconjuntos de A es

$$|\{0, 1\}^A| = 2^{|A|} = 2^m.$$

El método de conteo anterior funciona siempre que se pueda determinar que el conjunto dado puede escribirse como un producto cartesiano. Sin embargo, en la situación general esto no siempre es posible, y en muchos casos el conjunto viene dado sólo como un subconjunto de un producto cartesiano y en este caso necesitamos un principio de conteo general que nos ayude a contar estos conjuntos. A un subconjunto T del producto cartesiano $A \times B$ lo llamaremos también una *tabla*. La utilidad de estas tablas para nosotros vendrá en el hecho de que para contar los elementos de un conjunto que no viene definido por una lista, conviene en ocasiones poner este conjunto en una tabla. Comenzamos con un ejemplo para ilustrar las ideas involucradas:

Ejemplo 9. En uno de los cursos de álgebra se sabe que hay 12 alumnos hombres y que cada uno de ellos es amigo de exactamente 5 de sus condiscípulas. Si cada alumna es amiga de exactamente 4 compañeros, ¿cuántas alumnas hay en el curso?

Para resolver este problema, denotemos con A al conjunto de alumnos y por B al conjunto de alumnas. El hecho de que el alumno $a \in A$ sea amigo de la alumna $b \in B$ lo representamos mediante el par ordenado (a, b). Sabemos que $|A| = 12$, por lo que podemos listar sus elementos $A = \{a_1, a_2, \ldots, a_{12}\}$.

Con estos datos formamos la tabla T correspondiente, representando por un punto $\bullet$ cada uno de los pares (a, b) donde a es amigo de b:

	b_1	b_2	$\cdots$	b_n
a_1	$\bullet$		$\bullet$	
a_2		$\bullet$		
a_3				$\bullet$
$\vdots$				
a_m	$\bullet$			

Observemos que, fijo el alumno a, en el *renglón* de T que le corresponde se encuentran todas las alumnas b que son sus amigas. Así, al contar los puntos de este renglón tenemos al número de amigas del alumno a. Denotemos este número por R_a.

En forma similar, si fijamos a la alumna $b \in B$, en la *columna* de T que le corresponde se encuentran todos los alumnos que son sus amigos, de tal forma que al contar los puntos de esta columna se obtiene el número de amigos de la alumna b. Denotemos este número por C_b.

Ahora, es claro que para la tabla T se tiene que

$$|T| = \sum_{a \in A} R_a$$

y

$$|T| = \sum_{b \in B} C_b$$

ya que da lo mismo contar los puntos $\bullet$ de T recorriendo las columnas o recorriendo los renglones. Se tiene así que

$$\sum_{a \in A} R_a = \sum_{b \in B} C_b = |T|.$$

En nuestro ejemplo, cada R_a es constante 5 y cada C_b es constante 4. Se tiene entonces que:

$$|T| = \sum_{a \in A} R_a = \sum_{a \in A} 5 = 12 \times 5 = 60$$

(ya que sabemos que $|A| = 12$).

Pongamos $n = |B|$ (el número de alumnas). Entonces,

$$|T| = \sum_{b \in B} C_b = \sum_{b \in B} 4 = 4n$$

y por lo tanto

$$60 = |T| = 4n$$

por lo que $n = 15$, es decir, hemos contado el número de alumnas sin necesidad de listarlas.

El ejemplo siguiente ilustra el método general que obtendremos después:

Ejemplo 10. ¿De cuántas maneras se pueden poner las 4 llantas de un automóvil? En este ejemplo, estamos suponiendo que se tienen 4 llantas y que en el automóvil los lugares correspondientes están numerados (digamos, comenzando con la llanta delantera del lado del conductor y luego siguiendo el sentido de las manecillas del reloj). Podemos representar esto mediante una tabla con cuatro casillas, cada una representando el lugar correspondiente donde se pondrá uno de los objetos (en este caso, una llanta):

Pensamos que las casillas están numeradas de izquierda a derecha (en este caso del 1 al 4).

Ahora, cuando colocamos las llantas, digamos comenzando con la casilla 1, tenemos 4 llantas para elegir cuál ponemos en la casilla 1. Esto lo representamos por la tabla:

(4)			

Una vez colocada la llanta en la casilla 1, nos quedan 3 llantas para elegir una para la casilla 2; es decir, tenemos 3 elecciones posibles para la casilla 2. Esto lo representamos por la tabla:

(4)	(3)		

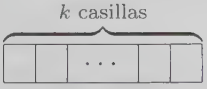
Y notamos que, por cada elección de la llanta de la casilla 1, tenemos 3 elecciones para la llanta en la casilla 2. Así, hay $(4)(3) = 12$ elecciones para colocar las primeras dos llantas.

Continuando de esta manera, una vez colocadas las llantas de las casillas 1 y 2, para la casilla 3 quedan 2 llantas para elegir. Y una vez hecho esto queda sólo una llanta para colocar en la casilla 4. La tabla correspondiente es:

(4)	(3)	(2)	(1)

Por lo tanto, hay (4)(3)(2)(1)=24 maneras de colocar las llantas en el automóvil.

Detengámonos unos momentos para analizar el razonamiento empleado en los dos conteos anteriores. En la situación general tenemos k casillas en las cuales debemos distribuir objetos de ciertos conjuntos finitos $A_1, \ldots, A_k$ dados,



bajo las condiciones siguientes: en la casilla 1 podemos elegir los objetos de n_1 maneras, luego para cada elección de un objeto en la casilla 1, en la casilla 2 hay n_2 elecciones posibles, etc., para enteros positivos $1 \leq n_1, n_2, \ldots, n_k \leq n$. Observemos ahora que, cada elección de un objeto $a_1 \in A_1$ en la casilla 1, un objeto $a_2 \in A_2$ en la casilla 2, etc., nos da una k-ada ordenada:

$$(a_1, a_2, \ldots, a_k) \in A_1 \times \cdots \times A_k,$$

de tal forma que lo que queremos es: si se sabe que hay n_1 maneras de elegir la primera componente a_1 de esta k-ada y que para cada elección de la primera componente hay n_2 maneras de elegir la segunda componente a_2, etc., la pregunta es: ¿de cuántas maneras se pueden elegir todas las k-adas ordenadas del problema dado? Notemos que, bajo las restricciones del problema en consideración, el conjunto de todas las k-adas ordenadas es sólo un subconjunto del producto cartesiano

$$A_1 \times \cdots \times A_k$$

y así no podemos usar los principios de multiplicación desarrollados hasta ahora. Sin embargo, quisiéramos justificar la intuición que nos dice que el número de maneras en las cuales podemos elegir todas las k-adas ordenadas del problema dado es el producto $n_1 n_2 \cdots n_k$.

Recopilando lo que tenemos hasta ahora: si

$$T \subseteq A_1 \times \cdots \times A_k$$

es un subconjunto del producto cartesiano de los conjuntos finitos $A_1, \ldots, A_k$ y si sabemos que hay n_1 elecciones posibles de las primeras componentes de T, esto significa que, si consideramos la función *proyección en la primera componente*

$$p_1 : T \subseteq A_1 \times \cdots \times A_k \longrightarrow A_1$$

(dada por $(a_1, a_2, \ldots, a_k) \mapsto a_1 \in A_1$), entonces el hecho de que haya n_1 elecciones posibles para las primeras componentes de T se expresa por la igualdad:

$$n_1 = |p_1(T)|.$$

El problema siguiente es: habiendo elegido la primera componente a_1, ¿cómo elegimos la segunda componente? Observemos que en este momento estamos considerando las dos primeras componentes de las k-adas de T, por lo que es natural considerar la *proyección en las primeras dos componentes*

$$p_2 : T \subseteq A_1 \times \cdots \times A_k \longrightarrow A_1 \times A_2$$

(dada por $(a_1, a_2, \ldots, a_k) \mapsto (a_1, a_2) \in A_1 \times A_2$) y el hecho de que, una vez elegida la primera componente $a_1 \in p_1(T)$ existan n_2 elecciones posibles para la segunda componente, se expresa por la igualdad

$$n_2 = |\{y \in A_2 : (a_1, y) \in p_2(T)\}|.$$

El problema siguiente es: habiendo elegido las dos primeras componentes $(a_1, a_2) \in p_2(T)$, ¿cómo elegimos la tercera componente? De nuevo, como estamos considerando ahora las tres primeras componentes de las k-adas de T, debemos pensar en la proyección en las tres primeras componentes

$$p_3 : T \subseteq A_1 \times \cdots \times A_k \longrightarrow A_1 \times A_2 \times A_3$$

(dada por $(a_1, a_2, a_3, \ldots, a_k) \mapsto (a_1, a_2, a_3) \in A_1 \times A_2 \times A_3$) y el hecho de que, una vez elegidas dos primeras componentes $(a_1, a_2) \in p_2(T)$ existan n_3 elecciones posibles para la tercera componente, se expresa por la igualdad

$$n_3 = |\{y \in A_3 \ : \ (a_1, a_2, y) \in p_3(T) \ \}|.$$

En general, necesitaremos, para cada $1 \leq j \leq k$, las proyecciones en los primeros j factores:

$$p_j : T \subseteq A_1 \times \cdots \times A_k \longrightarrow A_1 \times \cdots \times A_j \tag{1}$$

(dadas por $(a_1, \ldots, a_j, \ldots, a_k) \mapsto (a_1, \ldots, a_j) \in A_1 \times \cdots \times A_j$), de tal forma que el hecho de que, una vez elegidas primeras $j-1$ componentes $(a_1, a_2, \ldots, a_{j-1}) \in p_{j-1}(T)$ existan n_j elecciones posibles para la j-ésima componente, se expresa por la igualdad

$$n_j = |\{y \in A_j \ : \ (a_1, \ldots, a_{j-1}, y) \in p_j(T) \ \}|.$$

Con estas notaciones a la mano, podemos formular el problema de conteo que tenemos como sigue: si para cada elemento $(a_1, a_2, \ldots, a_k)$ de T, para la primera componente $a_1 \in p_1(T)$ hay n_1 formas de elegirlo, y una vez hecho lo anterior, para cada a_1 hay n_2 maneras de elegir la componente $a_2 \in A_2$ tal que $(a_1, a_2) \in p_2(T)$, y una vez hecho esto, para el par $(a_1, a_2) \in p_2(T)$ hay n_3 maneras de elegir $a_3 \in A_3$ de tal forma que $(a_1, a_2, a_3) \in p_3(T)$, etc., ¿cuántos elementos tiene T?

TEOREMA II.30 (Principio generalizado del producto). *Sean A_1, ..., A_k conjuntos finitos y T un subconjunto del producto cartesiano $A_1 \times \cdots \times A_k$. Supongamos que para cualquier $(a_1, \ldots, a_{j-1}) \in p_{j-1}(T)$ existen n_j elementos $y \in A_j$ tal que $(a_1, \ldots, a_{j-1}, y) \in p_j(T)$, entonces*

$$|T| = n_1 n_2 \cdots n_k,$$

donde $n_1 = |p_1(T)|$ y, para $j \geq 2$, $n_j = |\{y \in A_j \ : \ (a_1, \ldots, a_{j-1}, y) \in p_j(T) \ \}|$.

Demostración. Por inducción sobre $k \geq 2$.

(I) Para $k = 2$, $T \subseteq A_1 \times A_2$. Consideremos la proyección $p_1 : T \to A_1$ y observemos que $n_1 = |p_1(T)|$ por hipótesis. Ahora, para cada $a_i \in p_1(T)$ consideremos la columna

$$C_i = \{(a_i, b) \in T\}$$

donde notamos que, para cualesquiera a_i y $a_{i'}$ en $p_1(T)$ se tiene la biyección $C_i \to C_{i'}$ dada por $(a_i, b) \mapsto (a_{i'}, b)$, de tal forma que $|C_i|$ es constante. Más aún, por hipótesis, fijo el elemento $a_i \in p_1(T)$ se tiene que

$$|C_i| = n_2,$$

además es claro que $C_i \cap C_{i'} = \emptyset$ si $i \neq i'$ y $\bigcup_{a_i \in p_1(T)} C_i = T$, entonces, por el principio de la suma

$$|T| = \sum_{a_i \in p_1(T)} |C_i| = \sum_{a_i \in p_1(T)} n_2 = |p_1(T)| n_2,$$

por lo que $|T| = n_1 n_2$, como se requería.

(II) Supongamos el resultado válido para $k \geq 2$ y sea $T \subseteq A_1 \times \cdots \times A_k \times A_{k+1}$. Podemos pensar a las $(k+1)$-adas en T

$$(a_1, \ldots, a_k, a_{k+1}) = ((a_1, \ldots, a_k), a_{k+1}) = (a^{(k)}, a_{k+1})$$

como pares ordenados con $a^{(k)} := (a_1, \ldots, a_k) \in p_k(T)$. Ahora, para cada $a^{(k)} := (a_1, \ldots, a_k) \in p_k(T)$ fijo, la columna $C_k := \{(a^{(k)}, b) \in T\}$ tiene cardinal $|C_k| = n_{k+1}$ por hipótesis, y claramente $T = \bigcup_{a^{(k)} \in p_k(T)} C_k$, las columnas son disjuntas y tienen cardinal constante n_{k+1} (como en el caso $k = 2$), por lo que, usando el principio de la suma

$$|T| = \sum_{a^{(k)} \in p_k(T)} |C_k| = \sum_{a^{(k)} \in p_k(T)} n_{k+1} = |p_k(T)| n_{k+1},$$

y por hipótesis de inducción $|p_k(T)| = n_1 \cdots n_k$, por lo que

$$|T| = n_1 \cdots n_k n_{k+1},$$

como se quería. □

II.6.1 Ordenaciones y permutaciones

Dado un conjunto finito A con m elementos y un intervalo $\mathbb{I}_n$ de números naturales, como $\mathbb{I}_n = \{1, 2, \ldots, n\}$ y $A = \{a, b, c, \ldots\}$, a una función $f : \mathbb{I}_n \to A$ la podemos representar mediante un arreglo como el que sigue:

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a & b & c & \cdots & x \end{pmatrix}$$

donde en el primer renglón ponemos el dominio $\mathbb{I}_n$ y debajo de cada $j \in \mathbb{I}_n$ se pone el único elemento $t \in A$ tal que $t = f(j)$. Así en la representación de arriba tenemos que $f(1) = a$, $f(2) = b$, $f(3) = c, \ldots$, $f(n) = x$.

Si ahora recordamos que $\mathbb{I}_n \subseteq \mathbb{N}$ está ordenado (por el orden heredado de $\mathbb{N}$), una función $f : \mathbb{I}_n \to A$ es una lista o sucesión finita de n elementos (permitiendo repeticiones, porque la función no tiene que ser inyectiva) de A escogidos en el orden de $\mathbb{I}_n$. Diremos que una tal función f es una *n-ordenación con repetición* de elementos de A. En ocasiones también decimos que una n-ordenación con repetición es una *n-palabra* en el *alfabeto* A. Veamos algunos ejemplos:

Ejemplo 11. Si $A = \{a, e, i, o, u\}$ es el conjunto de vocales y $n = 3$, una función $f : \mathbb{I}_3 \to A$ es una lista con tres vocales (permitiendo repeticiones); por ejemplo:

$$\begin{pmatrix} 1 & 2 & 3 \\ a & i & e \end{pmatrix},$$

y como se permiten repeticiones, otro ejemplo es:

$$\begin{pmatrix} 1 & 2 & 3 \\ e & e & u \end{pmatrix}.$$

En ocasiones, para simplificar, escribimos sólo el segundo renglón en los arreglos anteriores, sobreentendiendo el dominio $\mathbb{I}_n$ correspondiente. Así, los ejemplos de arriba quedan:

$$(a, i, e) \quad \text{y} \quad (e, e, u),$$

o, escritas como 3-palabras:

$$aie \quad \text{y} \quad eeu.$$

Entonces, el problema de contar cuántas n-ordenaciones con repetición de un conjunto A que tiene cardinalidad m, es el problema de contar cuántas funciones $f : \mathbb{I}_n \to A$ hay. Denotemos este número con $OR(m, n)$. En (II.29) ya hemos calculado este número:

COROLARIO II.31. *Si A es un conjunto finito con m elementos, entonces el número de funciones $f : \mathbb{I}_n \to A$ es $OR(m, n) = m^n$.* □

Para su uso en el caso cuando queramos contar funciones inyectivas, veamos otra manera de calcular $OR(m, n)$, comenzando con unos casos especiales:

(I) Si $|A| = m$ y $n = 1$, queremos calcular $OR(m, 1)$, es decir, queremos calcular el número de funciones $f : \mathbb{I}_1 \to A$. Ahora, como $\mathbb{I}_1 = \{1\}$, es claro que cada elección de un elemento $a \in A$ nos da una función $f_a : \mathbb{I}_1 \to A$ tal que $f_a(1) = a$. Entonces, hay exactamente m funciones de $\mathbb{I}_1$ en A. Es decir, $OR(m, 1) = m$.

EJERCICIO 29. Use inducción sobre $m = |A|$ para dar una demostración formal de la afirmación anterior.

(II) Consideremos ahora $OR(m, 2)$, es decir, contemos el número de funciones $f : \mathbb{I}_2 \to A$. Como $\mathbb{I}_2 = \mathbb{I}_1 \cup \{2\}$, entonces una función $f : \mathbb{I}_2 \to A$ se puede pensar como una función $f_1 : \mathbb{I}_1 \to A$ a la que se extendió a $\mathbb{I}_2$ dándole un valor al $2 \in \mathbb{I}_2$, es decir, dando el valor $f(2) \in A$. Ahora, como este valor $f(2)$ puede ser cualquier elemento de A y hay precisamente m posibles valores para este elemento, entonces cada función $f_1 : \mathbb{I}_1 \to A$ se puede extender de m diferentes maneras a todo $\mathbb{I}_2$. Finalmente, como hay $OR(m, 1)$ funciones $f_1 : \mathbb{I}_1 \to A$ y cada una de éstas se puede extender a m diferentes funciones de $\mathbb{I}_2$ en A, entonces, por el principio generalizado del producto, hay $m \cdot OR(m, 1)$ funciones de $\mathbb{I}_2$ en A.

(III) En forma similar, para calcular $OR(m, 3)$ pensamos a $\mathbb{I}_3 = \mathbb{I}_2 \cup \{3\}$ y consideramos a las funciones $f : \mathbb{I}_3 \to A$ como extensiones de funciones $f_2 : \mathbb{I}_2 \to A$ dándoles a éstas el valor $f(3) \in A$ y observando de nuevo que hay m elecciones posibles para estos valores, por el principio generalizado del producto, cada función f_2 se puede extender de m diferentes maneras a todo $\mathbb{I}_3$. Se sigue que $OR(m, 3) = m \cdot OR(m, 2)$.

En el caso general, las funciones $f : \mathbb{I}_n \to A$ las vemos como extensiones de funciones $f_{n-1} : \mathbb{I}_{n-1} \to A$ a las que se les puede dar el valor $f(n) \in A$ de m maneras distintas, de tal forma que, por el principio generalizado del producto,

$$OR(m, n) = m \cdot OR(m, n-1).$$

Finalmente, como $OR(m, 1) = m$, las fórmulas anteriores nos dicen que

$$OR(m, n) = m^n.$$

Hemos así probado de nuevo el corolario anterior.

Supongamos ahora que queremos contar sólo las funciones inyectivas de un intervalo $\mathbb{I}_n$ de $\mathbb{N}$ en un conjunto finito A con m elementos. Para comenzar, por el ejercicio 18 se debe tener que $n \leq m$. Y notemos que como $f : \mathbb{I}_n \to A$ es ahora inyectiva, en las ordenaciones

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a & b & c & \cdots & x \end{pmatrix}$$

no se permiten repeticiones. A estas ordenaciones se les llamará simplemente *n-ordenaciones* sobreentendiendo que son sin repetición. Denotaremos con $\mathrm{O}(m, n)$ al número de n-ordenaciones de elementos de un conjunto A con cardinalidad m, *i.e.,* al número de funciones inyectivas $f : \mathbb{I}_n \to A$. Para calcular $\mathrm{O}(m, n)$ procedemos como en la segunda demostración para el caso de $OR(m, n)$:

(I) Para $\mathbb{I}_1 = \{1\}$, hay exactamente m funciones $f : \mathbb{I}_1 \to A$ necesariamente inyectivas por lo que $\mathrm{O}(m, 1) = m$.

(II) Para $\mathbb{I}_2 = \mathbb{I}_1 \cup \{2\}$, si $f_1 : \mathbb{I}_1 \to A$ es una función (necesariamente inyectiva), nos preguntamos de cuántas maneras se puede extender en forma inyectiva a todo $\mathbb{I}_2$, es decir, de cuántas maneras podemos definir $f(2) \in A$ de tal forma que la nueva función siga siendo inyectiva. Para esto, notamos que si $f_1(1) = a \in A$, entonces $f(2)$ no puede ser igual a a ya que la función debe ser inyectiva. Entonces $f(2)$ sólo puede tomar los otros $m - 1$ valores en A (exceptuando el $a \in A$ ya tomado); es decir, hay $(m - 1)$ extensiones inyectivas de f_1 a todo $\mathbb{I}_2$. Por el principio generalizado del producto se sigue que

$$\mathrm{O}(m, 2) = (m-1)\mathrm{O}(m, 1) = (m-1)m.$$

(III) Para $\mathbb{I}_3 = \mathbb{I}_2 \cup \{3\}$, dada una función inyectiva $f_2 : \mathbb{I}_2 \to A$, ¿de cuántas maneras se puede extender inyectivamente a $\mathbb{I}_3$? De nuevo, si $f_2(1) = a$ y $f_2(2) = b$, entonces $f(3)$ no puede ser igual ni a a ni a b. Así hay $(m-2)$ posibilidades para $f(3)$ en A, por lo que

$$\mathrm{O}(m,3) = (m-2)\mathrm{O}(m,2) = (m-2)(m-1)m.$$

En el caso general, donde requerimos que $n \leq m$, las funciones inyectivas $f : \mathbb{I}_n \to A$ las vemos como extensiones de funciones inyectivas $f_{n-1} : \mathbb{I}_{n-1} \to A$ a las que se les puede dar el valor $f(n) \in A$ de $(m - (n-1))$ maneras distintas, de tal forma que, por el principio generalizado del producto,

$$\mathrm{O}(m,n) = (m-(n-1))\cdot \mathrm{O}(m,n-1) = (m-(n-1))(m-(n-2))\cdots(m-1)m.$$

Hemos así probado el resultado siguiente:

PROPOSICIÓN II.32. *Si A es un conjunto finito con m elementos y $n \leq m$, entonces el número de funciones inyectivas $f : \mathbb{I}_n \to A$ es*

$$\mathrm{O}(m,n) = m(m-1)(m-2)\cdots(m-n+1). \qquad \square$$

Finalmente, supongamos que queremos contar el número de funciones biyectivas de un intervalo $\mathbb{I}_m$ en un conjunto A, que por (II.21) debe tener también m elementos. Esto es lo mismo que contar el número de funciones biyectivas de A en A. Una función biyectiva $f : A \to A$ se llamará una *permutación* de A. Recordemos ahora que, por (II.23), una función $f : A \to A$ es biyectiva si y sólo si es inyectiva. Ahora, por la proposición anterior, si $|A| = m$, el número de funciones inyectivas de $\mathbb{I}_m$ en A es

$$\mathrm{O}(m,n) = m(m-1)(m-2)\cdots(m-(m-1)) = m(m-1)(m-2)\cdots 2\cdot 1.$$

Al número $m(m-1)(m-2)\cdots 2\cdot 1$ se le llama el *factorial* del natural m y se le denota por $m!$; así, $m!$ es el producto de todos los naturales del 1 al m. Con esta notación y como consecuencia de la discusión anterior, hemos probado que:

PROPOSICIÓN II.33. *Si A es un conjunto finito con m elementos, entonces el número de permutaciones de A es $m!$.* $\square$

Con la notación factorial, el número de ordenaciones sin repetición $\mathrm{O}(m,n)$ se puede escribir como

$$\mathrm{O}(m,n) = \frac{m!}{(m-n)!},$$

con la convención de que, si $m = n$, $0! := 1$.

II.6.2 Combinaciones

Dado un conjunto finito A con n elementos, los subconjuntos $B \subseteq A$ con k elementos, $0 \leq k \leq n$, se llaman *combinaciones de k elementos de A.*

Ejemplo 12. Si $A = \{a, e, i, o, u\}$, entonces $n = |A| = 5$, y si $k = 4$, entonces los subconjuntos de A con cuatro elementos son

$$\{a, e, i, o\}, \{a, e, i, u\}, \{a, e, o, u\}, \{a, i, o, u\}, \{e, i, o, u\}$$

y hay 5 de estas combinaciones.

Si $k = 1$, las combinaciones de A con un elemento son:

$$\{a\}, \{e\}, \{i\}, \{o\}, \{u\}$$

y hay 5 de estas combinaciones.

Si $k = 5$, sólo hay un subconjunto de A con 5 elementos, a saber, A mismo.

Si $k = 0$, sólo hay un subconjunto de A con 0 elementos, a saber, el conjunto vacío.

EJERCICIO 30. Para el conjunto A del ejemplo anterior, encuentre los subconjuntos de A con $k = 3$ elementos. Encuentre también las combinaciones de 2 elementos de A.

EJERCICIO 31. Si A y B son finitos y $f : A \to B$ es una función suprayectiva tal que para todo $b \in B$ se tiene que $|f^{-1}(b)| = k$ (constante), demuestre que $|A| = k \cdot |B|$.

Si A es cualquier conjunto finito con $|A| = n$ elementos y $0 \leq k \leq n$, denotaremos con $\binom{n}{k}$ o $C(n,k)$ al número de combinaciones de k elementos del conjunto A que tiene n elementos. Para calcular este número, observemos que si

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & k \\ a_1 & a_2 & a_3 & \cdots & a_k \end{pmatrix}$$

es una ordenación de elementos de A tomados de k en k, entonces asociada a esta ordenación se tiene el subconjunto $\{a_1, a_2, \ldots, a_k\}$ de A, que tiene k elementos ya que una ordenación es una función inyectiva. Si denotamos con $\mathcal{O}_k(A)$ al conjunto de ordenaciones de k elementos de A y con $\mathcal{C}_k(A)$ al conjunto de combinaciones de k elementos de A, hemos definido así una función

$$\psi : \mathcal{O}_k(A) \to \mathcal{C}_k(A)$$

mediante

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & k \\ a_1 & a_2 & a_3 & \cdots & a_k \end{pmatrix} \mapsto \{a_1, \ldots, a_k\}.$$

Es claro que ψ es suprayectiva, ya que dado el subconjunto

$$A_k = \{a_1, \ldots, a_k\} \subseteq A,$$

como los a_i son distintos, se tiene la ordenación $f = (a_1, \ldots, a_k) \in \mathcal{O}_k(A)$ y obviamente $\psi(f) = A_k$. Observamos ahora que, para cada combinación $\{a_1, \ldots, a_k\}$ de k elementos de A, hay $k!$ ordenaciones que van a dar a la combinación dada (ya que $k!$ es el número de permutaciones del conjunto $\{a_1, \ldots, a_k\}$). En otras palabras, la imagen inversa $\psi^{-1}(A_k)$ de cada $A_k \in \mathcal{C}_k(A)$ tiene cardinal $|\psi^{-1}(A_k)| = k!$. Finalmente, como $\psi : \mathcal{O}_k(A) \to \mathcal{C}_k(A)$ es suprayectiva, las imágenes inversas $\psi^{-1}(A_k)$ de cada $A_k \in \mathcal{C}_k(A)$ forman una partición de $\mathcal{O}_k(A)$ y así, por el principio de la suma se tiene que

$$|\mathcal{O}_k(A)| = \sum_{A_k \in \mathcal{C}_k(A)} |\psi^{-1}(A_k)| = \sum_{A_k \in \mathcal{C}_k(A)} (k!) = |\mathcal{C}_k(A)|(k!) = \binom{n}{k}(k!),$$

y así hemos probado que

$$\mathrm{O}(n,k) = \#(\mathcal{O}_k(A)) = k! \cdot \#(\mathcal{C}_k(A)) = k! \cdot \binom{n}{k},$$

y como, por (II.30), $\mathrm{O}(n,k) = n(n-1)\cdots(n-k+1)$, entonces

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Ahora, si $k = 0$, se extiende en la forma acostumbrada la noción de factorial mediante $0! = 1$, y así, hemos probado:

TEOREMA II.34. *Si A es un conjunto finito con n elementos y $0 \leq k \leq n$, entonces el número de combinaciones de k elementos de A es*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \qquad \square$$

El triángulo de Pascal. Variando n y $0 \leq k \leq n$ listemos todos los coeficientes $C(n,k) = \binom{n}{k}$ correspondientes, organizándolos en una tabla:

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

$$\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5}$$

$$\bullet\bullet\bullet$$

En este arreglo observamos que en la dirección vertical ($\downarrow$) hacemos variar la n y en cada renglón tenemos todos los valores de k correspondientes: $0 \leq k \leq n$. Si calculamos los valores de $\binom{n}{k}$ en la tabla anterior, queda:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & \bullet\bullet\bullet & & & & &
\end{array}
$$

Lo primero que llama la atención en este arreglo es su simetría: cada renglón es simétrico con respecto a su centro:

PROPOSICIÓN II.35. $\binom{n}{k} = \binom{n}{n-k}$.

Demostración. Si A es un conjunto finito con n elementos, por cada subconjunto con k elementos se tiene su complemento con $n-k$ elementos, y así hay tantos subconjuntos con k elementos como subconjuntos con $n-k$ elementos. □

La segunda observación importante acerca del arreglo triangular anterior (llamado el *triángulo de Pascal*) es: en los extremos de cada renglón se encuentran los números $\binom{n}{0} = 1 = \binom{n}{n}$ y los otros $\binom{n}{k}$ se obtienen sumando los números que se encuentran inmediatamente arriba a la izquierda y derecha de $\binom{n}{k}$, es decir, de los números $\binom{n-1}{k-1}$ y $\binom{n-1}{k}$. Ésta es la fórmula básica de recurrencia del triángulo de Pascal:

TEOREMA II.36 (Fórmula básica de recurrencia en el triángulo de Pascal). *Si* $n \geq 2$, *entonces*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Demostración. Sea A un conjunto finito con n elementos y sea $1 \leq k \leq n$. Al considerar subconjuntos de A con k o $k-1$ elementos, sin perder generalidad podemos suponer que $A = \mathbb{I}_n$. Consideremos la familia $\mathcal{C}_k(\mathbb{I}_n)$ de subconjuntos de $\mathbb{I}_n$ con k elementos. Privilegiando al elemento $1 \in \mathbb{I}_n$ podemos separar los miembros de la familia $\mathcal{C}_k(\mathbb{I}_n)$ en dos clases disjuntas: los que contienen al 1 y los que no. Observemos ahora que para formar un subconjunto de $\mathbb{I}_n$ con k elementos y que contenga al 1, sólo necesitamos elegir $(k-1)$ elementos de los $n-1$ elementos restantes de $\mathbb{I}_n$ y así, hay $C(n-1,k-1)$ subconjuntos de $\mathbb{I}_n$ con k elementos y que contienen al 1. Ahora, los subconjuntos con k elementos de $\mathbb{I}_n$ y que no contienen al 1 se deben obtener de $\mathbb{I}_n - \{1\}$ y hay $C(n-1,k)$ de estos subconjuntos.

Finalmente, como el total de los k-subconjuntos de $\mathbb{I}_n$ es $C(n,k)$, por el principio de la suma aplicado a $\mathcal{C}_k(\mathbb{I}_n)$, que se ha separado en 2 clases disjuntas, se tiene que:

$$C(n,k) = C(n-1,k-1) + C(n-1,k). \qquad \square$$

EJERCICIO 32. Usando que un conjunto finito con n elementos tiene 2^n subconjuntos (ejemplo 8), demuestre que

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

EJERCICIO 33. Demuestre que

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

EJERCICIO 34. Para un valor dado de n, ¿cuáles valores de k hacen máximo el coeficiente binomial $\binom{n}{k}$?

La expansión binomial. Los números $C(n,k) = \binom{n}{k}$ son muy importantes en matemáticas y se suelen llamar *coeficientes binomiales* debido a que al considerar la expansión de un binomio $(1+x)^n$, para $n \geq 0$, estos números aparecen como los coeficientes del término x^k, como veremos en el teorema siguiente, donde también mostramos que la expansión de $(1+x)^n$ tiene $n+1$ términos.

TEOREMA II.37. *Si $(1+x)^n$ se desarrolla como una suma de potencias de x, el coeficiente de x^k es $C(n,k)$. Es decir,*

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = \sum_{k=0}^{n}\binom{n}{k}x^k.$$

Demostración. Basta con probar la primera afirmación, y para esto consideremos el producto

$$\overbrace{(1+x)(1+x)\cdots(1+x)}^{n \text{ factores}}$$

y observemos que, al desarrollar este producto, un término donde aparezca x^k se obtiene escogiendo k paréntesis $(1+x)$ y seleccionando el término x de cada uno de estos paréntesis, y finalmente se selecciona el término 1 de los restantes $(n-k)$ paréntesis. Así, en el desarrollo anterior, los términos x^k aparecen tantas veces como formas de elegir k paréntesis de los n paréntesis dados hay, *i.e.*, en $C(n,k)$ maneras, y por lo tanto éste es el coeficiente de x^k. □

Una generalización inmediata es:

TEOREMA II.38. *Si $n \geq 1$ es cualquier entero y a, b son dos símbolos que conmutan, i.e., $ab = ba$, entonces*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

Demostración. Es una variación de la demostración anterior: debemos ver que el coeficiente del término $a^{n-k}b^k$ es $C(n,k)$, y para esto observamos que del desarrollo

$$\overbrace{(a+b)(a+b)\cdots(a+b)}^{n \text{ factores}}$$

para elegir a^{n-k} debemos elegir $n-k$ factores $(a+b)$ y escoger al término a de cada uno de éstos y de los restantes k factores elegimos a b. Pero hay $C(n,n-k) = C(n,k)$ de estas elecciones (la igualdad por la simetría de los coeficientes binomiales (II.35)). □

EJERCICIO 35. Si a, b son reales y $b \neq 0$, dé otra demostración del teorema anterior usando el teorema (II.37).

Otro caso especial es:

COROLARIO II.39. *Si $n \geq 1$ es cualquier entero y a, b son dos símbolos que conmutan, i.e., $ab = ba$, entonces*

$$(a-b)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} a^{n-k} b^k.$$

Demostración. Se sigue del teorema anterior poniendo $-b$ en lugar de b. □

EJERCICIO 36. Usando la expansión binomial (II.37), dé otra demostración del ejercicio 32:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

Concluya que si A es un conjunto finito con n elementos, entonces el número de subconjuntos de A es 2^n.

Observación. Las propiedades que hemos usado de los coeficientes binomiales $C(n,k) = \binom{n}{k}$, en general no requieren el cálculo (II.34) de estos números y hay varias formas de obtener este cálculo, una de ellas se sugiere en el ejercicio 37, usando la proposición siguiente, que Fermat llamaba, en una carta a Roverbal y Mersenne en 1636, *une tres-belle proposition*:

PROPOSICIÓN II.40.

$$(n+1)\binom{n}{k} = (k+1)\binom{n+1}{k+1}.$$

Demostración. Sea A un conjunto finito de cardinalidad $|A| = n+1$ y sea $\wp(A)$ el conjunto potencia de A, *i.e.*, el conjunto de subconjuntos de A. Consideremos el conjunto

$$R = \{(a, T) \subseteq A \times \wp(A) \ : \ a \in T \ \text{ y } \ |T| = k+1\} \subseteq A \times \wp(A).$$

Note que el número de subconjuntos $T \subseteq A$ con $k+1$ elementos es $C(n+1, k+1)$, por lo que

$$|R| = (k+1)\binom{n+1}{k+1}.$$

Por otra parte, como $a \in T$, los otros k elementos de T se deben elegir de $A - \{a\}$ que tiene n elementos y, así, hay $C(n,k)$ de estos conjuntos para cada $a \in A$ fijo. Ahora, como $|A| = n+1$, por el principio del producto hay $(n+1)C(n,k)$ de estos pares (a,T), por lo que

$$|R| = (n+1)\binom{n}{k}.$$

Las dos igualdades anteriores implican el resultado deseado. □

EJERCICIO 37. Usando esta proposición, deduzca que

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

EJERCICIO 38. Por el teorema binomial

$$(1+x)^{n+1} = \sum_{k+1=0}^{n+1} \binom{n+1}{k+1} x^{k+1},$$

de donde, derivando, se obtiene que

$$(n+1)(1+x)^n = \sum_{k=1}^{n+1} (k+1)\binom{n+1}{k+1} x^k.$$

Comparando los coeficientes de x^k deduzca la proposición anterior.

EJERCICIO 39. Sea p un primo. Demuestre que $p|\binom{p}{k}$ para toda k tal que $1 \leq k \leq p-1$. Usando esto, demuestre, por inducción sobre n, que p divide a $n^p - n$.

EJERCICIO 40. Las llaves de una cerradura tienen un cierto número de partes que se pueden cortar a diferentes profundidades. Si hay 8 partes y 10 profundidades posibles, ¿cuántas llaves diferentes se pueden hacer?

EJERCICIO 41. De un grupo de 24 alumnos, ¿cuántos equipos de futbol se pueden formar? (Un equipo de futbol se forma con 11 personas.) Si uno de los 24 alumnos ha sido elegido capitán y siempre debe jugar, ¿de cuántas maneras se puede elegir el equipo?

EJERCICIO 42. Cada uno de los 5 días laborables de la semana puedo comprar uno de 4 periódicos que me gustan para leer en el Metro. ¿De cuántas maneras puedo hacer esto?

EJERCICIO 43. ¿De cuántas maneras pueden distribuirse $3n$ objetos en 3 cajas distintas, de modo que cada caja reciba n objetos?

EJERCICIO 44. ¿De cuántas maneras pueden repartirse 25 objetos entre cuatro personas?

EJERCICIO 45. De los 32 equipos de futbol que participan en el Mundial, al término del torneo quedan cuatro equipos semifinalistas que se disputan los primeros cuatro lugares.

(I) ¿De cuántas maneras pueden resultar las eliminatorias iniciales para determinar los primeros cuatro lugares?

(II) ¿De cuántas maneras pueden resultar las eliminatorias para determinar los primeros cuatro lugares, si el equipo de Brasil siempre debe ser uno de ellos?

II.6.3 El principio de inclusión-exclusión

Hemos visto, en secciones anteriores, la importancia del principio de la suma que, entre otras cosas, nos ha permitido obtener otros métodos de conteo que permiten resolver varios de estos problemas. En el ejercicio 25 se pidió demostrar la generalización del principio básico de la suma al caso cuando A_1 y A_2 son conjuntos finitos arbitrarios no necesariamente disjuntos:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Usando este ejercicio, la asociatividad de la unión y la distributividad de la intersección con respecto de la unión, se puede generalizar al caso de tres conjuntos finitos A_1, A_2, A_3, como sigue:

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |(A_1 \cup A_2) \cup A_3| \\ &= |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| \end{aligned}$$

$$
\begin{aligned}
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| \\
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - (|A_1 \cap A_3| + |A_2 \cap A_3| \\
&\quad - |A_1 \cap A_3 \cap A_2 \cap A_3|) \\
&= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\
&\quad + |A_1 \cap A_2 \cap A_3|.
\end{aligned}
$$

Así, poniendo

$$
\begin{aligned}
s_1 &= |A_1| + |A_2| + |A_3| \\
s_2 &= |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| \\
s_3 &= |A_1 \cap A_2 \cap A_3|
\end{aligned}
$$

la expresión anterior queda:

$$|A_1 \cup A_2 \cup A_3| = s_1 - s_2 + s_3.$$

El lector puede obtener la fórmula correspondiente para cuando se tienen cuatro conjuntos finitos A_1, A_2, A_3, A_4.

La idea detrás de estas fórmulas es que al contar los elementos que están en la unión $A_1 \cup \cdots \cup A_n$, si un elemento x pertenece a la intersección de algunos de los conjuntos (para fijar ideas pensemos que pertenece a todos los conjuntos A_i), cuando sumamos los cardinales $|A_1| + \cdots + |A_n|$, lo estamos contando n veces, es decir, lo estamos incluyendo n veces; para remediar esto consideramos todos los pares de conjuntos distintos y sus intersecciones $A_i \cap A_j$ con $i \neq j$ y restamos los cardinales $|A_i \cap A_j|$. Observemos que de los n conjuntos al escoger familias de dos conjuntos hay $C(n, 2)$ de estos conjuntos y así al substraer éstos estamos excluyendo $C(n, 2)$ veces al elemento x. De nuevo, quizá lo excluimos de más y así consideramos las intersecciones de tres conjuntos distintos $A_i \cap A_j \cap A_k$ y notamos que hay $C(n, 3)$ de estas ternas y entonces sumamos los cardinales de estas ternas incluyendo de nuevo al elemento x, y así sucesivamente.

Para simplificar la notación, observemos que, en general, dado k entre 1 y n, hay $C(n, k)$ familias con k conjuntos de los A_i y así pongamos

$$s_k := \sum |A_{j_1} \cap \cdots \cap A_{j_k}|$$

donde la suma recorre todas las $C(n, k)$ familias de k conjuntos A_j. El teorema siguiente recoge las observaciones anteriores:

TEOREMA II.41 (Principio de inclusión-exclusión). *Sea A un conjunto finito y sean $A_1, A_2, \ldots, A_n$ subconjuntos de A. Sean s_k, $1 \leq k \leq n$ como antes. Entonces,*

$$|A_1 \cup \cdots \cup A_n| = s_1 - s_2 + s_3 - s_4 + \cdots + (-1)^{n+1} s_n.$$

Demostración. Dado un elemento arbitrario $x \in A$, la idea es ver que, al ser contado, contribuye lo mismo en el lado izquierdo de la igualdad del teorema que en el lado derecho. Para comenzar, si $x \notin A_1 \cup \cdots \cup A_n$, entonces claramente x contribuye 0 a ambos lados de la igualdad del teorema. Supongamos que $x \in A_1 \cup \cdots \cup A_n$ y que, de hecho, x está en exactamente t de los conjuntos A_i. Entonces, $1 \leq t \leq n$, y x obviamente contribuye 1 al ser contado en la parte izquierda. Observemos ahora que si $k > t$, entonces x no contribuye a la suma s_k. Por otro lado, si $k \leq t$ entonces x aparece $C(t,k)$ veces en la suma s_k. Así, su contribución neta al lado derecho de la igualdad del teorema es:

$$C(t,1) - C(t,2) + C(t,3) - C(t,4) + \cdots + (-1)^{t+1} C(t,t),$$

que es igual a

$$\begin{aligned}
&= 1 - 1 + \binom{t}{1} - \binom{t}{2} + \binom{t}{3} - \binom{t}{4} + \cdots + (-1)^{t+1} \binom{t}{t} \\
&= \binom{t}{0} - \left\{ \binom{t}{0} - \binom{t}{1} + \binom{t}{2} - \binom{t}{3} + \cdots + (-1)^{t} \binom{t}{t} \right\} \\
&= 1 - \{(1-1)^t\} \\
&= 1,
\end{aligned}$$

que es lo se quería. □

Ejemplo 13. Un *desarreglo* de un conjunto finito A con n elementos es una permutación σ de A sin puntos fijos, es decir, $\sigma(a) \neq a$ para todo $a \in A$. Sin perder generalidad podemos suponer que $A = \mathbb{I}_n$ y así un desarreglo de $\mathbb{I}_n$ es una permutación de $\mathbb{I}_n$ tal que ningún número de $\mathbb{I}_n$ aparece en su posición inicial. Por ejemplo, $\sigma = (2,3,4,5,1)$ es un desarreglo de $\mathbb{I}_5$ pero $\tau = (2,3,5,4,1)$ no lo es ya que $\tau(4) = 4$. ¿Cuántos desarreglos tiene $\mathbb{I}_n$? Si denotamos con d_n este número, podemos listar sus primeros valores:

$d_1 = 0$ (ya que la única permutación de $\mathbb{I}_1$ es la identidad), $d_2 = 1$ ya que de las $2! = 2$ permutaciones de $\mathbb{I}_2$ una de ellas es la identidad y la otra es el desarreglo $(2, 1)$; $d_3 = 2$ ya que de las $3! = 6$ permutaciones de $\mathbb{I}_3$, se tienen los dos desarreglos $(2, 3, 1)$ y $(3, 1, 2)$.

Para poder calcular el número d_n de desarreglos de $\mathbb{I}_n$, observemos que las $n!$ permutaciones de $\mathbb{I}_n$ se dividen en dos clases: aquellas permutaciones que tienen algún punto fijo y los desarreglos, y vamos a contar el número de permutaciones de $\mathbb{I}_n$ que tienen algún punto fijo, *i.e.*, aquellas permutaciones σ para las cuales existe un $i \in \mathbb{I}_n$ tal que $\sigma(i) = i$. Nótese que pueden existir permutaciones σ que fijan un elemento de $\mathbb{I}_n$, o que fijan dos elementos, o que fijan tres elementos, ..., o que fijan n elementos. Denotemos con $F(i)$ al número de permutaciones que fijan al elemento $i \in \mathbb{I}_n$; entonces

$$F(i) = (n-1)! \tag{1}$$

ya que al estar i fijo los otros $(n-1)$ elementos de $\mathbb{I}_n$ se pueden permutar arbitrariamente entre sí.

Ahora, como también hay permutaciones que fijan dos elementos, digamos $i, j \in \mathbb{I}_n$, si denotamos por $F(i, j)$ al número de éstas, entonces

$$F(i, j) = (n-2)! \tag{2}$$

ya que al estar i y j fijos, los otros $(n-2)$ elementos de $\mathbb{I}_n$ se pueden permutar arbitrariamente entre sí.

Similarmente, el número de permutaciones que dejan fijos a tres elementos i, j, k de $\mathbb{I}_n$ es

$$F(i, j, k) = (n-3)! \tag{3}$$

y en forma análoga se obtiene el número de permutaciones de $\mathbb{I}_n$ que fijan m elementos dados de $\mathbb{I}_n$.

Observe ahora que hay $\binom{n}{1}$ maneras de escoger un elemento $i \in \mathbb{I}_n$ por lo que de (1) se sigue que hay

$$(n-1)!\binom{n}{1}$$

permutaciones que dejan fijo a un elemento de $\mathbb{I}_n$. Similarmente, hay $\binom{n}{2}$ maneras de elegir dos elementos de $\mathbb{I}_n$ y así, por (2), hay

$$(n-2)!\binom{n}{2}$$

permutaciones que fijan dos elementos de $\mathbb{I}_n$. Y, en general, si $k \leq n$, hay

$$(n-k)!\binom{n}{k}$$

permutaciones que fijan k elementos de $\mathbb{I}_n$.

Por el principio de inclusión-exclusión, el número de permutaciones de $\mathbb{I}_n$ que fijan algún elemento de $\mathbb{I}_n$ es

$$(n-1)!\binom{n}{1} - (n-2)!\binom{n}{2} + (n-3)!\binom{n}{3} - \cdots + (-1)^{n+1}(n-n)!\binom{n}{n}$$

por lo que el número de desarreglos de $\mathbb{I}_n$ es

$$\begin{aligned} d_n &= n! - \left((n-1)!\binom{n}{1} - (n-2)!\binom{n}{2} + \cdots + (-1)^{n+1}(n-n)!\binom{n}{n}\right) \\ &= n! - \left(\frac{(n-1)!n!}{1!(n-1)!} - \frac{(n-2)!n!}{2!(n-2)!} + \cdots + (-1)^{n+1}\frac{(n-n)!n!}{n!(n-n)!}\right) \\ &= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!}\right) \\ &= n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}. \end{aligned}$$

EJERCICIO 46. Si d_n es el número de desarreglos de $\mathbb{I}_n$, con $d_1 = 0$, $d_2 = 1$, obtenga la fórmula de recurrencia:

$$d_n = (n-1)d_{n-1} + (n-1)d_{n-2}, \qquad \text{si } n > 2.$$

EJERCICIO 47. En una clase de música con 73 alumnos hay 52 que tocan el piano, 25 el violín, 20 la flauta, 17 tocan piano y violín, 12 piano y flauta, 7 violín y flauta y 1 toca los tres instrumentos. ¿Hay algún alumno que no toque ninguno de los tres instrumentos?

EJERCICIO 48. Un comité de 8 personas se debe formar de un grupo de 10 chilenos y 15 argentinos. ¿De cuántas maneras se puede elegir este comité si:

(I) debe contener 4 personas de cada nacionalidad?

(II) debe haber más chilenos que argentinos?

(III) debe haber al menos dos chilenos?

EJERCICIO 49. De un grupo de 16 personas de Argentina, Brasil, Chile y México, se deben elegir 6 para representarlos en un comité. ¿Cuántas selecciones se pueden hacer si:

(I) cada país debe estar representado?

(II) ningún país puede tener más de dos representantes?

EJERCICIO 50. ¿Cuántos números telefónicos de 8 cifras hay, que inicien con el número 5513?

EJERCICIO 51. Suponga que las placas de los automóviles de la ciudad de México se forman por 3 letras seguidas de 3 cifras. Si no hay restricción sobre las letras y cifras, ¿cuántas placas se pueden formar? (El alfabeto consta de 26 letras.)

EJERCICIO 52. Si una cierta asociación consta de 40 personas y se quiere elegir una comisión formada por un presidente, un secretario y un tesorero, ¿de cuántas maneras se puede escoger esta comisión?

EJERCICIO 53. Considere un polígono regular de n lados. ¿Cuántas diagonales se pueden trazar en este polígono?

EJERCICIO 54. Una *sucesión binaria de longitud* n es una n-ordenación con repetición formada con 0 y 1.

(I) ¿Cuántas sucesiones binarias de longitud n hay?

(II) Liste todas las sucesiones binarias de longitud 4.

(III) ¿Cuántas sucesiones binarias de longitud $n = p + q$ se pueden formar si estas sucesiones deben contener p ceros y q unos, con $q \geq p - 1$, y además no deben tener dos ceros juntos?

EJERCICIO 55. La *distancia* entre dos sucesiones binarias de longitud n es el número de lugares en los cuales difieren. Por ejemplo, para las 3-sucesiones binarias 110 y 011 su distancia es 2 ya que sólo difieren en el primer y tercer lugares.

(I) Fija una sucesión binaria de longitud n, ¿cuántas n-sucesiones binarias distan d de ella?

(II) Obtenga una fórmula para el número de n-sucesiones binarias que distan $\leq e$ de una n-sucesión fija.

EJERCICIO 56. Seis personas deben ser sentadas en una mesa circular.

(I) ¿De cuántas maneras se pueden acomodar?

(II) ¿De cuántas maneras se pueden acomodar si A no quiere estar sentado junto a B?

EJERCICIO 57. Considere un conjunto N que contiene cinco enteros positivos ≤ 9. Demuestre que existen, al menos, dos subconjuntos de N cuyos elementos suman lo mismo.

EJERCICIO 58. ¿Cuántas palabras de longitud 3 (sin repetir signos) pueden formarse con un alfabeto de 256 letras, si requerimos que nunca aparezcan dos determinados signos (por ejemplo, las letras a y b) juntas?

EJERCICIO 59. Por un cierto canal de comunicación se va a transmitir un mensaje usando 12 símbolos diferentes. Además de estos 12 símbolos, el transmisor enviará un total de 45 espacios en blanco entre los símbolos con tres espacios como mínimo entre cada par de símbolos consecutivos. ¿De cuántas maneras se puede mandar el mensaje?

EJERCICIO 60. Demuestre que en cualquier grupo de 6 personas, o hay 3 que se conocen entre sí o hay 3 que son mutuamente desconocidas.

EJERCICIO 61. La sección escolar informa que cada alumno de una determinada licenciatura está inscrito en cuatro de las siete asignaturas que se ofrecen y las listas de alumnos por asignaturas tienen 52, 30, 30, 20, 25, 12 y 18 alumnos respectivamente. ¿Qué conclusión puede obtenerse de esta información?

EJERCICIO 62. ¿Cuántos enteros hay entre 1 y 1000 que no sean divisibles ni por 2 ni por 3 ni por 5?

EJERCICIO 63. ¿Cuántos enteros positivos menores que 10 000 son coprimos con 3 780? *Sugerencia: use el principio de inclusión-exclusión.*

EJERCICIO 64. Para $n \geq 2$, sea u_n el número de palabras de longitud n que se pueden formar con el alfabeto $\{0, 1\}$ y con la propiedad de no tener dos ceros consecutivos. Demuestre que

$$u_2 = 3, \quad u_3 = 4, \quad u_n = u_{n-1} + u_{n-2} \quad \text{para } n \geq 4.$$

EJERCICIO 65. ¿Cuántos números telefónicos de 8 dígitos tienen un dígito que aparece más de una vez?

II.7 PROYECTO 1: RECURRENCIA Y FUNCIONES GENERADORAS

En el ejemplo 4 de este capítulo, consideramos el problema de las torres de Hanoi y mostramos que el menor número de movidas $T(n)$ para llevar n discos de la torre A a la torre B, usando como intermediaria la torre C, estaba dada por la *fórmula recursiva*

$$T(n) = 2T(n-1) + 1.$$

Luego, observando que $T(1) = 1$, obtuvimos la *fórmula cerrada*

$$T(n) = 2^n - 1,$$

que después probamos por inducción.

En general, hay muchos problemas de conteo, como el del ejemplo anterior, que al resolverlos dan lugar a una fórmula recursiva. Otro ejemplo interesante es el siguiente:

Ejemplo 14. Supongamos que se tiene una pareja de conejos recién nacidos y que éstos maduran después de 1 mes y producen sus primeros hijos después de otro mes y de aquí en adelante tendrán un par de conejos cada mes. Denotemos al par recién nacido por A, después de 1 mes, cuando ya están maduros denotamos a la pareja por B y cuando ya tienen 2 meses y tienen hijos denotamos la pareja por C. Así, comenzando con un par de conejos recién nacidos, el crecimiento de una familia de conejos está dada como en la tabla siguiente:

Al mes 0	A	1 par
Al mes 1	B	1 par
Al mes 2	CA	2 pares
Al mes 3	CBA	3 pares
Al mes 4	CCBAA	5 pares
Al mes 5	CCCBBAAA	8 pares
Al mes 6	CCCCCBBBAAAAA	13 pares

EJERCICIO 66. Si denotamos con s_n al número de pares de conejos después de n meses, demuestre que

$$s_n = s_{n-1} + s_{n-2} \qquad \text{para } n \geq 2,$$

¡se supone que no desaparecen los conejitos! y los términos iniciales de la sucesión son $s_0 = 1 = s_1$.

Hemos recobrado la *sucesión de Fibonacci* del ejercicio 6, y de nuevo notamos que esta sucesión de enteros está dada por una fórmula recursiva: $s_n = s_{n-1} + s_{n-2}$, con las condiciones iniciales $s_0 = 1 = s_1$. En el ejercicio 6 se sugería cómo obtener una fórmula cerrada para la sucesión de Fibonacci:

$$s_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} \qquad \text{para } n \geq 2$$

donde α y β son las raíces de la ecuación cuadrática $x^2 = x + 1$.

Varias observaciones son relevantes con respecto a este ejemplo: primero, a pesar de que s_n es entero, en la fórmula cerrada anterior aparecen cocientes y raíces cuadradas; de alguna forma éstas deben cancelarse para al final dar lugar a un entero. Una pregunta pertinente sería: ¿cuál es el papel de la ecuación cuadrática en la deducción de la fórmula cerrada anterior?

Otro ejemplo similar es el siguiente:

EJERCICIO 67. Cierto microorganismo toma 1 hora para madurar y en otra hora ya produce 2 descendientes, repitiendo lo mismo cada hora subsecuente y lo mismo hacen sus descendientes. Comenzando con 1 microorganismo recién nacido, denotemos con b_n el número de microorganismos después de n horas. Calcule los primeros términos de esta sucesión. Demuestre que $b_n = b_{n-1} + 2b_{n-2}$, para $n \geq 3$.

EJERCICIO 68. Modifique el problema anterior suponiendo que cada microorganismo se muere después de producir su primer par de descendientes.

Los tres ejemplos anteriores dan lugar a sucesiones recurrentes de la forma

$$s_n = As_{n-1} + Bs_{n-2}, \qquad (n \geq 2)$$

con A y B constantes no cero y el problema es hallar una fórmula cerrada para s_n. El resultado general para estas fórmulas recurrentes es una generalización de la correspondiente para la sucesión de Fibonacci:

TEOREMA II.42 (Sucesiones tipo Fibonacci). *Supongamos que se tiene una sucesión recurrente de la forma*

$$s_n = As_{n-1} + Bs_{n-2}, \qquad (n \geq 2)$$

con A y B constantes no cero y los términos iniciales s_0 y s_1 dados. Considere la ecuación cuadrática

$$x^2 = Ax + B.$$

(1) *Si las raíces α, β de la ecuación $x^2 = Ax + B$ son distintas, entonces*

$$s_n = K_1\alpha^n + K_2\beta^n,$$

donde las constantes K_1 y K_2 están unívocamente determinadas por s_0 y s_1, A y B.

(2) *Si $x^2 = Ax + B$ tiene una sola raíz doble α,*

$$s_n = (K_1 + nK_2)\alpha^n,$$

donde las constantes K_1 y K_2 están unívocamente determinadas por s_0 y s_1, A y B.

Demostración. (1) Como la ecuación cuadrática tiene 2 raíces diferentes α y β, entonces para $n = 0$ y $n = 1$, las ecuaciones

$$s_0 = K_1\alpha^0 + K_2\beta^0$$
$$s_1 = K_1\alpha^1 + K_2\beta^1$$

determinan K_1 y K_2:

$$K_1 = \frac{s_1 - s_0\beta}{\beta - \alpha} \qquad \text{y} \qquad K_2 = \frac{s_1 - s_0\alpha}{\alpha - \beta}.$$

Note que $\alpha - \beta \neq 0$ porque $\alpha \neq \beta$ y además $\alpha \neq 0$ y $\beta \neq 0$ ya que $B \neq 0$. Por lo tanto, para estos valores de K_1 y K_2 la fórmula se verifica para $n = 0, 1$. Supongamos ahora que la fórmula es válida para índices $< n$ y verifiquémosla para n:

$$\begin{aligned}
s_n &= As_{n-1} + Bs_{n-2} \\
&= A(K_1\alpha^{n-1} + K_2\beta^{n-1}) + B(K_1\alpha^{n-2} + K_2\beta^{n-2}) \\
&= K_1(A\alpha^{n-1} + B\alpha^{n-2}) + K_2(A\beta^{n-1} + B\beta^{n-2}) \\
&= K_1\alpha^{n-2}(A\alpha + B) + K_2\beta^{n-2}(A\beta + B) \\
&= K_1\alpha^{n-2}(\alpha^2) + K_2\beta^{n-2}(\beta^2) \text{ (ya que como } \alpha \text{ y } \beta \text{ son raíces} \\
&\qquad \text{de } x^2 = Ax + B, \text{ entonces } A\alpha + B = \alpha^2 \text{ y } A\beta + B = \beta^2) \\
&= K_1\alpha^n + K_2\beta^n
\end{aligned}$$

que es lo que se quería.

(2) Como α es raíz múltiple de $x^2 = Ax + B$, entonces $x^2 - Ax - B = (x - \alpha)^2 = x^2 - 2\alpha x + \alpha^2$, de tal forma que $A = 2\alpha$ y $B = -\alpha^2$, y como $A \neq 0$, entonces $\alpha \neq 0$ también. Ahora, las ecuaciones

$$\begin{aligned}
s_0 &= K_1 = (K_1 + 0K_2)\alpha^0 \\
s_1 &= (K_1 + K_2)\alpha^1
\end{aligned}$$

determinan K_1 y K_2:

$$K_1 = s_0 \qquad \text{y} \qquad K_2 = \frac{s_1}{\alpha} - s_0,$$

y por lo tanto, para estos valores de K_1 y K_2 la fórmula se verifica para $n = 0, 1$. Supongamos ahora que la fórmula es válida para índices $< n$ y verifiquémosla para n:

$$\begin{aligned}
s_n &= As_{n-1} + Bs_{n-2} \\
&= A(K_1 + (n-1)K_2)\alpha^{n-1} + B(K_1 + (n-2)K_2)\alpha^{n-2} \\
&= K_1(A\alpha^{n-1} + B\alpha^{n-2}) + nK_2(A\alpha^{n-1} + B\alpha^{n-2}) - AK_2\alpha^{n-1} - 2BK_2\alpha^{n-2} \\
&= (K_1 + nK_2)(A\alpha^{n-1} + B\alpha^{n-2}) - \alpha^{n-2}K_2(A\alpha + 2B) \\
&= (K_1 + nK_2)\alpha^{n-2}(A\alpha + B) - \alpha^{n-2}K_2(A\alpha + 2B) \\
&= (K_1 + nK_2)\alpha^{n-2}(\alpha^2) - \alpha^{n-2}K_2(2\alpha^2 - 2\alpha^2),
\end{aligned}$$

ya que $A\alpha + B = \alpha^2$, $A = 2\alpha$ y $B = -\alpha^2$. Se sigue que $s_n = (K_1 + nK_2)\alpha^n$, como se quería. □

Ejemplo 15. Para la sucesión de Fibonacci, $s_0 = 1$, $s_1 = 1$ y $s_n = s_{n-1} + s_{n-2}$ (si $n \geq 2$), se tiene que $A = 1 = B$, por lo que la ecuación cuadrática asociada es $x^2 = x + 1$, cuyas raíces son

$$\alpha = \frac{1}{2}(1 + \sqrt{5}) \qquad \text{y} \qquad \beta = \frac{1}{2}(1 - \sqrt{5}),$$

por lo que, de acuerdo al teorema anterior,

$$s_n = K_1 \left(\frac{1 + \sqrt{5}}{2}\right)^n + K_2 \left(\frac{1 - \sqrt{5}}{2}\right)^n$$

y como $s_0 = 1$ y $s_1 = 1$, entonces las constantes K_1 y K_2 se obtienen resolviendo el sistema de ecuaciones:

$$s_0 = 1 = K_1\alpha^0 + K_2\beta^0$$
$$s_1 = 1 = K_1\alpha^1 + K_2\beta^1$$

que nos da:

$$K_1 = \frac{1}{\sqrt{5}}\alpha \qquad \text{y} \qquad K_2 = -\frac{1}{\sqrt{5}}\beta,$$

de tal forma que la fórmula cerrada buscada es:

$$s_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2}\right)^{n+1}.$$

EJERCICIO 69. Sea s_n el número de n-sucesiones binarias, para $n \geq 2$, véase el ejercicio 54, donde no se permite que aparezcan dos ceros consecutivos. Demuestre que $s_2 = 3$, $s_3 = 4$ y que $s_n = s_{n-1} + s_{n-2}$, para $n \geq 4$. Encuentre una fórmula cerrada para s_n.

EJERCICIO 70. Encuentre una fórmula cerrada para la sucesión de recurrencia del ejercicio 67: $b_n = b_{n-1} + 2b_{n-2}$, para $n \geq 2$, con las condiciones iniciales $b_0 = 1$, $b_1 = 2$.

EJERCICIO 71. Encuentre una fórmula cerrada para la sucesión de recurrencia del ejercicio 68.

El teorema anterior tiene varias limitaciones, por ejemplo, no incluye la sucesión recurrente obtenida en el problema de las torres de Hanoi. Otro ejemplo no incluido es el siguiente:

Ejemplo 16. Se tienen k pelotas iguales y se desea pintar cada una de ellas con un color de n colores dados. ¿De cuántas maneras es posible colorearlas?

Denotemos el número de maneras de colorear las pelotas por $p(n, k)$ ya que depende del número de colores disponibles n y del número de pelotas k. Veamos primero algunos casos extremos:

(I) Si sólo hay un color, $n = 1$, entonces las k pelotas sólo se pueden pintar de este color. Así

$$p(1, k) = 1 \qquad \text{para todo } k \geq 1.$$

(II) Si hay n colores y una sola pelota, $k = 1$, entonces esta pelota se puede pintar usando cualquiera de los n colores disponibles, *i.e.*,

$$p(n, 1) = n \qquad \text{para todo } n \geq 1.$$

Además, si n y k son pequeños, podemos intentar listar todas las posibilidades, por ejemplo, si hay $k = 3$ pelotas y $n = 2$ colores, digamos verde $= \oplus$ y rojo $= \otimes$, las posibilidades son:

$$\oplus\oplus\oplus$$
$$\oplus\oplus\otimes$$
$$\oplus\otimes\otimes$$
$$\otimes\otimes\otimes$$

por lo que $p(2, 3) = 4$.

Similarmente, si hay $k = 2$ pelotas y $n = 2$ colores (verde y rojo como antes), las posibilidades son:

$$\oplus\oplus$$
$$\oplus\otimes$$
$$\otimes\otimes$$

por lo que $p(2, 2) = 3$.

El problema es encontrar una fórmula para $p(n,k)$. La idea es reducir el problema a uno con menos pelotas o colores. Con este fin, al pintar las k bolas separemos las posibilidades en dos familias disjuntas: cuando se usa el color n y cuando no se usa el color n. Cuando no se usa el color n las k pelotas se pintaron usando $n-1$ colores y las combinaciones posibles son $p(n-1,k)$. Cuando se usa el color n, al menos alguna pelota se ha pintado usando este color n, y si la quitamos nos quedan $k-1$ pelotas que, usando los n colores, se pueden pintar de $p(k-1,n)$ maneras. Finalmente, como las dos familias de posibilidades son disjuntas y cubren todas las posibilidades de pintar todas las pelotas, por el principio de la suma se tiene que

$$p(n,k) = p(n-1,k) + p(n,k-1).$$

Ésta es una *fórmula recursiva* para el problema de coloración que consideramos. Los casos extremos (I) y (II) son las *condiciones de frontera* del problema y, de nuevo, lo que queremos es una *fórmula cerrada* para $p(n,k)$ y notamos que este caso no está incluido en las sucesiones tipo Fibonacci.

Para obtener esta fórmula cerrada, pensemos al problema de pintar k pelotas con n colores como un proceso mediante el cual el conjunto de k pelotas se separa en n subconjuntos (alguno de los cuales puede ser vacío) cada uno formado por pelotas pintadas iguales de uno de los n colores. Así, si numeramos estos n subconjuntos, digamos que el primer subconjunto tiene t_1 pelotas pintadas del color 1, el segundo subconjunto tiene t_2 pelotas pintadas del color 2, ..., el n-ésimo subconjunto tiene t_n pelotas pintadas del color n, de tal forma que los enteros satisfacen que $t_i \geq 0$ (son cero cuando el conjunto correspondiente es vacío) y además

$$t_1 + t_2 + \cdots + t_n = k.$$

Cada una de las elecciones de coloración la podemos representar como una tabla:

donde los cuadros □ indican que tenemos un cambio de color. Obsérvese que hay exactamente $(n-1)$ cambios de color. Nótese también que el número total de círculos es k. Así, en la tabla de arriba hay un total de $(n-1)+k$ celdas posibles que pueden ser llenadas con k círculos o $(n-1)$ cuadrados. Obsérvese también que la tabla está determinada una vez que elegimos las

posiciones de los cambios de colores, *i.e.*, una vez que elegimos del total $n+k-1$ de celdas las posiciones de los $n-1$ cuadrados. Es decir, $p(n,k)$ es el número de formas de elegir $n-1$ celdas del total de $n+k-1$ celdas:

$$p(n,k) = \binom{n+k-1}{n-1}.$$

Ésta es la fórmula cerrada que estábamos buscando para $p(n,k)$. Sin embargo, el problema da para más: en el proceso anterior obtuvimos la ecuación

$$t_1 + t_2 + \cdots + t_n = k$$

de tal manera que $p(n,k)$ es el número de soluciones en enteros no negativos ($t_i \geq 0$) de la ecuación anterior.

Con esto en mente, consideremos el producto siguiente:

$$\overbrace{(1+x+x^2+\cdots)(1+x+x^2+\cdots)\cdots(1+x+x^2+\cdots)}^{n \text{ factores}}$$

y preguntemos: ¿cuál será el coeficiente de x^k una vez que este producto se haya desarrollado?

Notemos que al expandir el producto anterior, el término x^k aparece cada vez que escogemos x^{t_1} en el primer paréntesis, x^{t_2} en el segundo paréntesis, $\ldots$, x^{t_n} en el n-ésimo paréntesis, de tal manera que

$$x^{t_1}x^{t_2}\cdots x^{t_n} = x^k,$$

por lo que la única condición es que

$$t_1 + t_2 + \cdots + t_n = k.$$

Así, el coeficiente de x^k en la expansión anterior es precisamente $p(n,k)$:

$$p(n,k) = \text{coeficiente de } x^k \text{ en } (1+x+x^2+\cdots)^n.$$

Si ahora recordamos que

$$1 + x + x^2 + \cdots = \frac{1}{1-x} = (1-x)^{-1},$$

entonces hemos mostrado que

$$p(n,k) = \text{coeficiente de } x^k \text{ en } (1-x)^{-n}.$$

EJERCICIO 72. Otro ejemplo de una sucesión de recurrencia que no es del tipo Fibonacci es la sucesión $a_n = na_{n-1}$, con la condición inicial $a_1 = 1$. ¿Reconoce esta sucesión?

EJERCICIO 73. Considere la sucesión de recurrencia dada por $a_1 = 2$ y, para $n \geq 2$, $a_n = a_{n-1} + 2n$. Demuestre que $a_n = n(n+1)$.

EJERCICIO 74. Otro ejemplo es la sucesión $a_n = n^2 a_{n-1}$, con $a_1 = 1$. ¿Reconoce esta sucesión?

Expansiones binomiales con exponentes negativos. En (II.37) y (II.39) consideramos expansiones binomiales de la forma $(1+x)^n$ y $(1-x)^n$ con n un entero positivo y mostramos que

$$(1 \pm x)^n = 1 \pm nx \pm \frac{n(n-1)}{2!}x^2 \pm \frac{n(n-1)(n-2)}{3!}x^3 \cdots \pm x^n.$$

El problema anterior nos ha llevado a considerar potencias binomiales con exponentes enteros negativos $(1-x)^{-n}$ y hemos visto que

$$(1-x)^{-n} = (1 + x + x^2 + x^3 + \cdots)^n$$

de tal manera que, a diferencia del caso con exponentes enteros no negativos de (II.37) y (II.39), el desarrollo binomial anterior no será una suma finita y se tiene una *serie*:

$$(1-x)^{-n} = (1 + x + x^2 + x^3 + \cdots)^n = \sum_{k=0}^{\infty} p(n,k)x^k = \sum_{k=0}^{\infty} \binom{n+k-1}{n-1} x^k,$$

donde los coeficientes de x^k son los números $p(n,k)$ como probamos anteriormente.

Resumiendo, en esta reinterpretación del problema de coloración anterior, los números $p(n,k)$ aparecen como los coeficientes de x^k en la serie de potencias

$$(1-x)^{-n} = \sum_{k=0}^{\infty} p(n,k)x^k,$$

y decimos que la función $f(x) = (1-x)^{-n}$ es la *función generadora* de los números $p(n,k)$.

En general, si $a_0, a_1, a_2, \ldots$, es una sucesión de números reales o complejos, la *función generadora* asociada es la serie

$$f(x) = \sum_{k=0}^{\infty} a_k x^k$$

con la convención de que $x^0 = 1$, de tal forma que a_k es el coeficiente de x^k en la serie anterior. De esta forma la función generadora $f(x)$ empaca todos los números a_k.

Ejemplo 17. Si consideramos los números $a_k = 1/k!$ para $k \geq 0$, la función generadora correspondiente es la *función exponencial*:

$$\exp(x) = \sum_{k=0}^{\infty} \frac{1}{k!} x^k.$$

Ejemplo 18. Si $a_n = (-1)^{n-1}/n$, la función generadora es el *logaritmo natural*:

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n.$$

Ejemplo 19. Para la sucesión de Fibonacci s_n, la función generadora

$$s(x) = \sum_{n=0}^{\infty} s_n x^n = x + x^2 + 2x^3 + 3x^4 + 5x^5 + \cdots$$

satisface que

$$\sum_{n=0}^{\infty} s_{n+2} x^{n+2} = \sum_{n=0}^{\infty} (s_{n+1} + s_n) x^{n+2} = \sum_{n=0}^{\infty} s_{n+1} x^{n+2} + \sum_{n=0}^{\infty} s_n x^{n+2}$$

de donde se sigue que

$$s(x) - x = x s(x) + x^2 s(x)$$

por lo que

$$(1 - x - x^2) s(x) = x$$

y así

$$s(x) = \frac{x}{1 - x - x^2}$$

es la función generadora de la sucesión de Fibonacci.

Obsérvese que, si α y β son las raíces de $1 - x - x^2$, entonces

$$s(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \alpha x)(1 - \beta x)} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \alpha x} - \frac{1}{1 - \beta x} \right),$$

de donde se sigue que

$$s_n = \frac{1}{\sqrt{5}} \left(\alpha^{n+1} - \beta^{n+1} \right).$$

Ejemplo 20. Las expansiones binomiales, para los exponentes enteros que hemos visto hasta ahora, tienen la forma

$$(1 + x)^n = 1 + nx + \frac{n(n-1)}{2!} x^2 + \frac{n(n-1)(n-2)}{3!} x^3 + \cdots$$

donde la suma es finita (con $n + 1$ términos) si $n \geq 0$ y es infinita si $n < 0$. De hecho, la expansión binomial anterior también es válida si n no es un entero, lo cual se sugiere al lector que verifique en cualquier libro de Análisis. Por ejemplo, para $n = 1/2$ la expansión binomial tiene la forma:

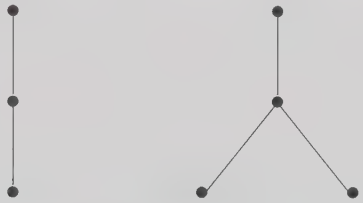
$$(1 + x)^{1/2} = 1 + \frac{1}{2} x + \frac{1}{2} (-\frac{1}{2}) \frac{1}{2!} x^2 + \frac{1}{2} (-\frac{1}{2}) (-\frac{3}{2}) \frac{1}{3!} x^3 + \cdots,$$

donde, para $k \geq 2$, el coeficiente de x^k es:

$$\begin{aligned} (-1)^{k+1} \frac{1 \cdot 3 \cdot 5 \cdots (2k-3)}{2^k \cdot k!} &= \frac{(-1)^{k+1} (2k-2)!}{2^k \cdot k! \cdot 2 \cdot 4 \cdots (2k-2)} \\ &= \frac{(-1)^{k+1} (2k-2)!}{2^k \cdot k! 2^{k-1} \cdot (k-1)!} \\ &= \frac{(-1)^{k+1} (2k-2)!}{2^{2k-1} \cdot k! \cdot (k-1)!}. \end{aligned}$$

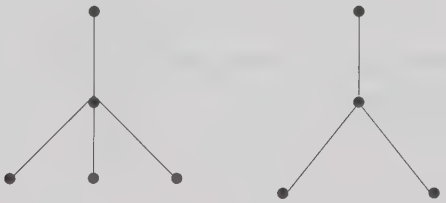
Observación. No hemos dicho nada acerca de qué tipo de funciones son las anteriores (¡o si son o no funciones!), es decir, si las series correspondientes convergen o no en un cierto dominio, o si las x son reales o complejos. El manejo que damos aquí es formal y, para las importantes cuestiones anteriores, referimos al lector a un buen libro de Análisis real o complejo.

Ejemplo 21. Una *gráfica plana* consta de un conjunto finito de *vértices* y un conjunto finito de *aristas* que unen algunos de los vértices. Una gráfica es *conexa* si cualesquiera dos vértices de ella se pueden conectar siguiendo aristas de la gráfica. En las gráficas que consideraremos no permitimos que existan dos aristas uniendo los mismos dos vértices. Un *ciclo* en una gráfica lo forma un conjunto de aristas que comienza y termina en el mismo vértice. Un *árbol* es una gráfica conexa sin ciclos. Los ejemplos siguientes son árboles:



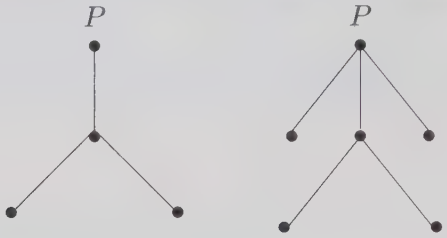
y las gráficas siguientes no son árboles:

La manera en que se guardan archivos en directorios de una computadora da lugar a árboles como los considerados arriba. En el ejemplo que consideraremos contaremos el número de ciertos árboles con número de vértices dado. Los árboles que contaremos son del tipo siguiente: un *árbol binario* es un árbol en el cual cada vértice tiene a lo más tres aristas (que salen o llegan al vértice). En la figura siguiente el primero no es un árbol binario y el segundo sí lo es:



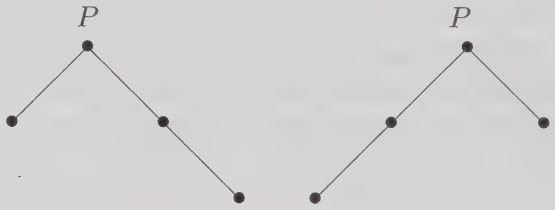
Un *árbol arraigado* es un árbol en el cual se ha distinguido un vértice P, llamado *raíz*, con la propiedad de que de este vértice sólo salen a lo más dos

aristas y no llega ninguna otra. Siempre consideraremos a la raíz P en la parte superior del árbol y por definición si P es una raíz, de P sólo emanan a lo más dos aristas. En la figura siguiente el primero es un árbol arraigado y el segundo no lo es:

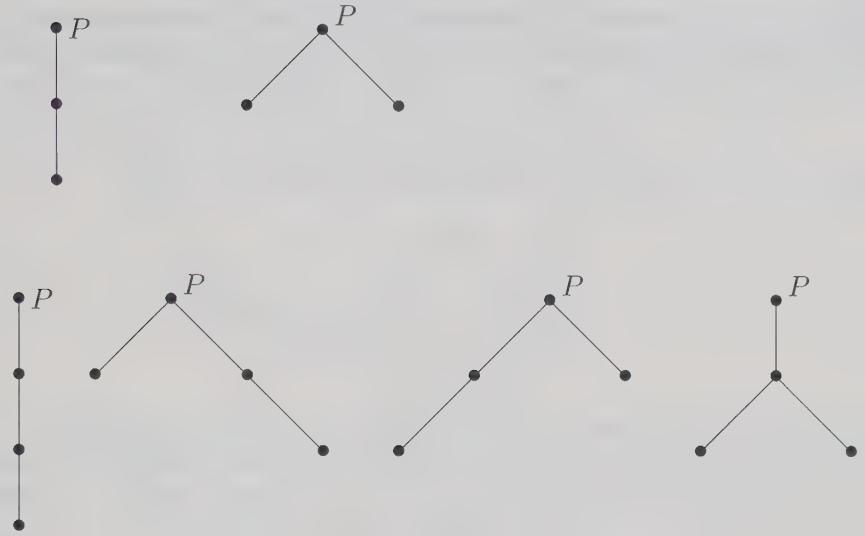


El problema que consideraremos ahora es contar el número a_n de árboles binarios arraigados con n vértices.

El primer problema que nos encontramos es típico de combinatoria: decidir cuándo dos árboles son diferentes. Para simplificar el problema nosotros pensaremos a los árboles como gráficas en el plano, de tal forma que, por ejemplo, los dos árboles siguientes serán considerados diferentes a pesar de que podemos *levantar* uno de ellos en el espacio y sobreponerlo en el otro. Sin embargo, no hay ninguna transformación adecuada en el plano que lleve uno de estos árboles en el otro:



Para n pequeño podemos listar todos los árboles binarios arraigados con n vértices. Los primeros ejemplos son:



De esta lista se tiene que: $a_1 = 1$, $a_2 = 1$, $a_3 = 2$, $a_4 = 4$.

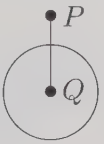
EJERCICIO 75. Liste los árboles correspondientes a a_5 y a_6 para calcular estos números.

Para contar el número a_n de árboles binarios arraigados con n vértices, separamos este conjunto en dos familias disjuntas: sea u_n el número de árboles con una sola arista saliendo de la raíz P y sea d_n el número de árboles con dos aristas saliendo de la raíz P. Por ejemplo, en la lista que hicimos antes para $n = 4$, el primer y cuarto árbol son del tipo 1 y los dos de en medio son del tipo 2. Por el principio de la suma se tiene que

$$a_n = u_n + d_n \quad \text{para } n \geq 2. \tag{1}$$

Así, para calcular a_{n+1} debemos calcular u_{n+1} y d_{n+1}.

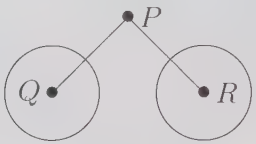
Para u_{n+1}: un árbol que contribuya a u_{n+1} es de la forma



donde, dentro del círculo, hay un árbol binario con n vértices arraigado en Q. Por hipótesis de inducción hay a_n de esos árboles y consecuentemente

$$u_{n+1} = a_n. \tag{2}$$

Para d_{n+1}: un árbol que contribuya a d_{n+1} es de la forma



donde en cada uno de los dos círculos hay un árbol binario arraigado en Q o en R respectivamente, y el árbol arraigado en Q tiene q vértices (digamos) y el árbol arraigado en R tiene r vértices, de tal forma que $q + r = n$. Así, para cada uno de los a_q árboles arraigados en Q hay a_r árboles arraigados en R y por lo tanto hay $a_q a_r$ árboles arraigados en Q y R para cada par de enteros $q, r \geq 1$ tales que $q + r = n$. Se sigue que

$$d_{n+1} = a_1 a_{n-1} + a_2 a_{n-2} + \cdots + a_{n-1} a_n = \sum_{q+r=n} a_q a_r. \tag{3}$$

De (1), (2) y (3) se sigue que

$$a_{n+1} = u_{n+1} + d_{n+1} = a_n + \sum_{q+r=n} a_q a_r$$

y por lo tanto la fórmula recursiva buscada es:

$$a_n = a_{n-1} + (a_1 a_{n-2} + a_2 a_{n-3} + \cdots + a_{n-2} a_1). \tag{4}$$

El problema es encontrar una fórmula cerrada para a_n. Para esto, consideremos las funciones generadoras asociadas a a_n, u_n y d_n:

$$a(x) = \sum_{n=1}^{\infty} a_n x^n = x + x^2 + 2x^3 + 4x^4 + \cdots$$

$$u(x) = \sum_{n=1}^{\infty} u_n x^n = x^2 + x^3 + 2x^4 + 4x^5 + \cdots$$

$$d(x) = \sum_{n=1}^{\infty} d_n x^n = x^3 + 2x^4 + \cdots$$

(donde en la segunda igualdad se tiene que $u_1 = 0$, $u_2 = 1$, $u_3 = 1$, $u_4 = 2$, lo cual puede verse de la tabla que hicimos de los ejemplos de arriba o puede deducirse de $u_{n+1} = a_n$. Similarmente, los coeficientes iniciales de la tercera igualdad se obtienen de los ejemplos listados antes).

Ahora, como $a_n = u_n + d_n$, se sigue que

$$a(x) = x + u(x) + d(x) \tag{5}$$

y como $u_{n+1} = a_n$, entonces

$$u(x) = xa(x) \tag{6}$$

(ya que el producto por x desplaza los exponentes de x^n un lugar a la derecha). También, como $d_{n+1} = \sum_{q+r=n} a_q a_r$, entonces

$$d(x) = x(a(x))^2 \tag{7}$$

(ya que $(a(x))^2$ da los coeficientes $a_q a_r$, para $q + r = n$, de d_{n+1} y el producto por x los desplaza un lugar). Las ecuaciones (5), (6) y (7) implican que

$$a(x) = x + u(x) + d(x) = x + xa(x) + x(a(x))^2,$$

es decir,

$$x(a(x))^2 + (x-1)(a(x)) + x = 0,$$

la cual es una ecuación cuadrática en la variable $a(x)$. Resolviendo esta ecuación obtenemos:

$$a(x) = \frac{1}{2x}\left[-(x-1) \pm \sqrt{(x-1)^2 - 4x^2}\right] = \frac{1}{2x}\left[1 - x \pm \sqrt{1 - (2x + 3x^2)}\right]$$

por lo que, usando el teorema del binomio para el exponente $1/2$:

$$(1-y)^{1/2} = 1 - \frac{1}{2}y - \frac{\frac{1}{2}\frac{1}{2}}{2!}y^2 - \frac{\frac{1}{2}\frac{1}{2}\frac{3}{2}}{3!}y^3 - \cdots - \frac{1 \cdot 3 \cdot 5 \cdots (2n-3)}{2^n n!}y^n + \cdots \tag{8}$$

y poniendo $y = 2x + 3x^2$, observando que queremos valores positivos para $s(x)$ por lo que el signo $(-)$ de (8) debe ser cancelado tomando el signo $(-)$ en las raíces que dan $s(x)$, obtenemos

$$s(x) = \frac{1}{2x}\left[1 - x - \left(1 - (2x + 3x^2)\right)^{1/2}\right]$$
$$= \frac{1}{2x}\left[-x + \frac{1}{2}(2x + 3x^2) + \frac{1}{2^2 \cdot 2!}(2x + 3x^2)^2 + \frac{3}{2^3 \cdot 3!}(2x + 3x^2)^3 \right.$$
$$\left. + \cdots + \frac{1 \cdot 3 \cdot 5 \cdots (2n-3)}{2^n n!}(2x + 3x^2)^n + \cdots\right]$$

que es la función generadora de a_n, lo cual, desde un cierto punto de vista resuelve el problema combinatorio inicial ya que los números a_n son los coeficientes de x^n en la serie anterior. En ocasiones, uno quiere más que lo anterior y el ejercicio siguiente va en esa dirección:

EJERCICIO 76. Escriba el coeficiente de y^n en la expansión binomial de $(1-y)^{1/2}$ de la forma:

$$a_n = \frac{1 \cdot 3 \cdot 5 \cdots (2n-3)}{2^n n!} = \frac{(2n-2)!}{2^{2n-1} n!(n-1)!}$$

y encuentre una fórmula para a_{n-1} en términos de n y a_n.

EJERCICIO 77. Encuentre la sucesión a_n cuya función generadora es

$$f(x) = \frac{1}{2}(e^x + e^{-x}).$$

EJERCICIO 78. Si $a_n = c$ (constante), encuentre la función generadora correspondiente.

Observación. En general, dada una función $f(x) = \sum_{n=0}^{\infty} a_n x^n$, el teorema de Taylor nos dice que $a_n = (1/n!) f^{(n)}(0)$, para $n \geq 0$ y donde $f^{(n)}$ es la n-ésima derivada de $f(x)$. Así, el problema de hallar la sucesión correspondiente a una función dada, es relativamente sencillo. Sin embargo, el problema inverso, *i.e.*, dada una sucesión a_n, hallar una fórmula explícita para la función generadora $f(x) = \sum_{n=0}^{\infty} a_n x^n$ en términos de funciones elementales, en general es muy difícil.

II.8 Bibliografía

[1] Rincón, H., *Cuando cuentes cuántos*, Temas de Matemáticas para Bachillerato, Instituto de Matemáticas, UNAM, México, 2002.

[2] Verde-Star, L., *Matemática discreta y combinatoria*, Anthropos, Barcelona, 1996.

III. EL ANILLO DE NÚMEROS ENTEROS

Los números naturales se pueden sumar y multiplicar, pero no se puede hacer *restas* con ellos, por ejemplo $2 - 5 \notin \mathbb{N}$, es decir, no existe un número natural x tal que $x + 5 = 2$. Para poder resolver ecuaciones tan simples como la anterior es necesario añadir al conjunto $\mathbb{N}$ los *números negativos* y el *cero* 0. Los números así obtenidos se llaman *números enteros* (positivos, negativos y el cero). La idea de la construcción de estos nuevos números es pensar a cada entero como una diferencia de naturales, *i.e.,* como $m - n$ con $m, n \in \mathbb{N}$. Ahora, como en $\mathbb{N}$ no existe la operación de resta, entonces pensaremos a $m - n$ como a un par ordenado $(m, n) \in \mathbb{N} \times \mathbb{N}$. Así, dados dos pares ordenados $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$, si pensamos al par (a, b) como $a - b$ y al par (c, d) como $c - d$, si queremos que sean iguales, *i.e.,* que $a - b = c - d$, como no hay resta en $\mathbb{N}$, entonces mejor escribimos la igualdad anterior como $a + d = b + c$ donde involucramos sólo operaciones permitidas en $\mathbb{N}$. Con esta idea como motivación se introduce la relación siguiente en $\mathbb{N} \times \mathbb{N}$:

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a + d = b + c.$$

Lema III.1. *La relación anterior en* $\mathbb{N} \times \mathbb{N}$ *es una relación de equivalencia.*

Demostración. La reflexividad y simetría son fáciles. Para la transitividad supongamos que $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$. Entonces $a + d = b + c$ y $c + f = d + e$. Sumando f en la primer igualdad y sumando b en la segunda igualdad se tiene que: $a + d + f = b + c + f$ y $b + c + f = b + d + e$, de donde se sigue que $a + d + f = b + d + e$ y cancelando d se sigue que $a + f = b + e$, *i.e.,* $(a, b) \sim (e, f)$. □

Ejercicio 1. Demuestre la reflexividad y simetría en el lema anterior.

El conjunto cociente $\mathbb{N} \times \mathbb{N}/\sim$ se denota $\mathbb{Z}$ y sus elementos, que son clases de equivalencia de pares ordenados $(a, b) \in \mathbb{N} \times \mathbb{N}$, se llaman *enteros* y los denotaremos mediante $[a, b]$.

III.1 Operaciones en $\mathbb{Z}$

En el conjunto cociente $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ se tienen operaciones de suma y producto de enteros, definidas como sigue: sean $[a,b], [c,d] \in \mathbb{Z}$ y escojamos representantes $(a,b) \in [a,b]$ y $(c,d) \in [c,d]$:

Suma. Una vez elegidos los representantes anteriores se "suman" como sigue:

$$(a,b) + (c,d) := (a+c, b+d)$$

y luego se toma la clase de equivalencia $[a+c, b+d] \in \mathbb{Z}$. Por supuesto que hay que probar que esta "definición" no depende de la elección de los representantes en cada clase. Esto se hará en la primera parte del siguiente lema.

Producto. Con los representantes anteriores se define

$$(a,b)(c,d) := (ac+bd, ad+bc)$$

(la idea es pensar a (a,b) como $a-b$ y a (c,d) como $c-d$ de tal forma que $(a-b)(c-d) = (ac+bd) - (ad+bc)$); después se toma la clase de equivalencia $[ac+bd, ad+bc] \in \mathbb{Z}$. Que ésta es una buena definición es el contenido de la segunda parte del lema siguiente:

Lema III.2. *Si* $(a,b) \sim (a',b')$ *y* $(c,d) \sim (c',d')$, *entonces:*

(1) $(a+c, b+d) \sim (a'+c', b'+d')$.

(2) $(ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c')$.

Demostración. (1) Por hipótesis $a+b' = b+a'$ y $c+d' = d+c'$. Entonces

$$\begin{aligned}(a+c)+(b'+d') &= (a+b')+(c+d') \\ &= (b+a')+(d+c') \quad \text{usando las hipótesis} \\ &= (b+d)+(a'+c') \quad \text{asociatividad y conmutatividad en } \mathbb{N}\end{aligned}$$

i.e., $(a+c, b+d) \sim (a'+c', b'+d')$.

Para la parte (2), multiplicando la igualdad de la primera hipótesis por d queda:

$$bd + a'd = ad + b'd, \tag{1}$$

multiplicando la igualdad de la primera hipótesis por c queda:

$$ac + b'c = bc + a'c, \tag{2}$$

multiplicando la igualdad de la segunda hipótesis por a' queda:

$$a'c + a'd' = a'd + a'c', \tag{3}$$

y multiplicando la igualdad de la segunda hipótesis por b' queda:

$$b'd + b'c' = b'c + b'd'. \tag{4}$$

Sumando estas cuatro igualdades:

$$(ac + bd) + (a'd' + b'c') + (a'd + b'c + a'c + b'd) =$$
$$(ad + bc) + (a'c' + b'd') + (b'd + a'c + a'd + b'c),$$

y cancelando el término del tercer paréntesis se sigue la igualdad deseada:

$$(ac + bd) + (a'd' + b'c') = (ad + bc) + (a'c' + b'd'). \qquad \square$$

Este lema nos dice que las operaciones:

$$[a, b] + [c, d] = [a + c, b + d]$$

y

$$[a, b][c, d] = [ac + bd, ad + bc],$$

están bien definidas en $\mathbb{Z}$. Para obtener las propiedades esperadas de estas operaciones necesitaremos el lema siguiente:

LEMA III.3. *Para cualesquiera números naturales a, b se cumple que:*

(1) $(a, a) \sim (b, b)$.

(2) $(a + 1, a) \sim (b + 1, b)$.

Demostración. (1) $a + b = a + b$ por la reflexividad de la igualdad.

(2) $(a + 1) + b = a + (b + 1)$ por la asociatividad y conmutatividad de la suma en $\mathbb{N}$. $\square$

TEOREMA III.4. *Las operaciones de suma y producto de* $\mathbb{Z}$ *satisfacen las propiedades siguientes:*

(1) *La suma es asociativa, i.e., para todo* $[a,b],[c,d],[e,f] \in \mathbb{Z}$ *se tiene que*

$$[a,b] + ([c,d] + [e,f]) = ([a,b] + [c,d]) + [e,f].$$

(2) *La suma es conmutativa, i.e., para todo* $[a,b],[c,d] \in \mathbb{Z}$ *se tiene que*

$$[a,b] + [c,d] = [c,d] + [a,b].$$

(3) *Existe un elemento neutro para la suma, llamado el cero,* $0 \in \mathbb{Z}$ *tal que*

$$[a,b] + 0 = [a,b] \qquad \text{para todo } [a,b] \in \mathbb{Z}.$$

(4) *Cada elemento* $[a,b] \in \mathbb{Z}$ *tiene un inverso aditivo, es decir, para* $[a,b] \in \mathbb{Z}$ *existe otro elemento* $[a',b'] \in \mathbb{Z}$ *tal que* $[a,b] + [a',b'] = 0$.

(5) *El producto es asociativo, i.e., para todo* $[a,b],[c,d],[e,f] \in \mathbb{Z}$ *se tiene que*

$$[a,b]([c,d][e,f]) = ([a,b][c,d])[e,f].$$

(6) *El producto es conmutativo, i.e., para todo* $[a,b],[c,d] \in \mathbb{Z}$ *se tiene que*

$$[a,b][c,d] = [c,d][a,b].$$

(7) *Existe un elemento neutro para el producto, llamado el uno,* $1 \in \mathbb{Z}$ *tal que*

$$1 \cdot [a,b] = [a,b] \qquad \text{para todo } [a,b] \in \mathbb{Z}.$$

(8) *Se cumple la ley distributiva: para todo* $[a,b],[c,d],[e,f] \in \mathbb{Z}$ *se tiene que*

$$[a,b]([c,d] + [e,f]) = [a,b][c,d] + [a,b][e,f].$$

Demostración. Ya hemos visto que $\mathbb{Z}$ es cerrado con respecto a las operaciones anteriores.

Asociatividad de la suma. Sean $[a,b],[c,d],[e,f] \in \mathbb{Z}$; entonces

$$\begin{aligned}
[a,b] + ([c,d] + [e,f]) &= [a,b] + [c+e, d+f] && \text{por definición de suma} \\
&= [a + (c+e), b + (d+f)] && \text{por definición de suma} \\
&= [(a+c)+e, (b+d)+f] && \text{asociatividad de suma en } \mathbb{N} \\
&= [a+c, b+d] + [e,f] && \text{por definición de suma} \\
&= ([a,b] + [c,e]) + [e,f] && \text{por definición de suma.}
\end{aligned}$$

Conmutatividad de la suma. Si $[a,b],[c,d] \in \mathbb{Z}$, entonces:

$$\begin{aligned}[a,b]+[c,d] &= [a+c,b+d] \\ &= [c+a,b+d] \quad \text{conmutatividad de la suma en } \mathbb{N} \\ &= [c,d]+[a,b].\end{aligned}$$

Neutro aditivo. Un neutro aditivo de $\mathbb{Z}$ es el entero $[s,s]$, para cualquier $s \in \mathbb{N}$, ya que para todo $[a,b] \in \mathbb{Z}$ se tiene que

$$[a,b]+[s,s] = [a+s,b+s] = [a,b]$$

la última igualdad porque $(a+s,b+s) \sim (a,b)$. Denotamos a la clase $[s,s] =: 0$.

Inversos aditivos. Un inverso aditivo del entero $[a,b] \in \mathbb{Z}$ es el entero $[b,a]$ ya que

$$[a,b]+[b,a] = [a+b,b+a] = [a+b,a+b] = [s,s] = 0$$

la penúltima igualdad porque $(m,m) \sim (n,n)$. Denotaremos al inverso aditivo de $[a,b]$ como $-[a,b] := [b,a]$.

Que el producto es asociativo, conmutativo y distribuye a la suma lo dejamos como ejercicio. El neutro multiplicativo de $\mathbb{Z}$ es la clase $[s+1,s]$ para cualquier $s \in \mathbb{N}$ ya que para cualquier $[a,b] \in \mathbb{Z}$:

$$\begin{aligned}[a,b][s+1,s] &= [a(s+1)+bs, as+b(s+1)] && \text{por definición de producto} \\ &= [as+a+bs, as+bs+b] && \text{(distributividad y asociatividad en } \mathbb{N}) \\ &= [a,b] && \text{porque } (a,b) \sim (a+t,b+t).\end{aligned}$$

Denotaremos a la clase $[s+1,s] =: 1$. □

Ejercicio 2. Demuestre la asociatividad y conmutatividad del producto en $\mathbb{Z}$.

Ejercicio 3. Demuestre que el producto distribuye a la suma en $\mathbb{Z}$.

Ejercicio 4. Demuestre la unicidad del elemento neutro aditivo en $\mathbb{Z}$, es decir, demuestre que si 0 y $0'$ son dos neutros aditivos en $\mathbb{Z}$, entonces $0 = 0'$.

Al neutro aditivo de $\mathbb{Z}$ (que es único por este ejercicio) lo denotamos con 0. Éste es el único elemento de $\mathbb{Z}$ que satisface que

$$a + 0 = a \qquad \forall a \in \mathbb{Z}.$$

Ejercicio 5. Demuestre la unicidad de los inversos aditivos en $\mathbb{Z}$, es decir, demuestre que si $a \in \mathbb{Z}$ y a' y a'' son dos inversos aditivos de a en $\mathbb{Z}$, entonces $a' = a''$.

Al inverso aditivo de $a \in \mathbb{Z}$ lo denotaremos mediante $-a$. Éste es el único (por el ejercicio anterior) elemento de $\mathbb{Z}$ tal que

$$a + (-a) = 0 \qquad \forall a \in \mathbb{Z}.$$

Ejercicio 6. Demuestre que el inverso aditivo del inverso aditivo de un elemento es el elemento dado, *i.e.*, demuestre que para todo $a \in \mathbb{Z}$ se tiene que $-(-a) = a$.

Ejercicio 7. Demuestre que el neutro multiplicativo de $\mathbb{Z}$ es único.

Al neutro multiplicativo de $\mathbb{Z}$ (que es único por este ejercicio) lo denotamos con 1. Este es el único elemento de $\mathbb{Z}$ que satisface que

$$a \cdot 1 = a \qquad \forall a \in \mathbb{Z}.$$

- Un conjunto A junto con dos operaciones, suma $(+)$ y producto $(\cdot)$ *cerradas* (es decir, la suma y producto de dos elementos de A es de nuevo un elemento de A) que satisfaga las propiedades (1), (2), (3), (4), (5) y (8) del teorema anterior, se dice que es un *anillo*. Si el anillo $(A, +, \cdot)$ además satisface la propiedad (6), *i.e.*, la conmutatividad del producto, diremos que se tiene un *anillo conmutativo*. Si el anillo $(A, +, \cdot)$ satisface la propiedad (7), *i.e.*, si tiene neutro multiplicativo, diremos que se tiene un *anillo con uno*.

- Con esta nomenclatura decimos que $(\mathbb{Z}, +, \cdot)$ es un *anillo conmutativo con uno*.

- Por supuesto que pueden existir anillos no conmutativos y anillos sin uno, pero en este libro sólo encontraremos anillos conmutativos con uno.

La resta. Como todos los elementos de un anillo A tienen inverso aditivo, se puede definir una operación de *resta* o *diferencia* en A como sigue: sean $a, b \in A$. Se define

$$a - b := a + (-b) \in A,$$

donde $-b$ denota el inverso aditivo de b.

A continuación probaremos algunas propiedades familiares de las operaciones aritméticas de $\mathbb{Z}$; nótese que en la demostración que daremos solamente se usan las propiedades de anillo conmutativo con uno, establecidas para $\mathbb{Z}$ en (III.4), y *no* se usa la definición de $\mathbb{Z}$ como conjunto cociente de una relación de equivalencia particular. Por lo tanto, las propiedades siguientes son válidas para cualquier anillo conmutativo con uno:

PROPOSICIÓN III.5. (1) *Para todo* $a \in \mathbb{Z}$ *se tiene que* $a \cdot 0 = 0$.

(2) $a(-b) = -(ab)$.

(3) $(-a)b = -(ab)$.

(4) $(-a)(-b) = ab$.

(5) $(-1)a = -a$.

Las propiedades (2), (3) y (4) son las llamadas *reglas de los signos*. Note que la propiedad (5) significa: *el inverso aditivo de* a *es el producto de* -1 *por* a.

Demostración. (1) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ (la primera igualdad porque $0 = 0 + 0$ y la segunda igualdad usando la distributividad). Sumando ahora el inverso aditivo de $a \cdot 0$ a ambos lados de la igualdad anterior se sigue que:

$$\begin{aligned} 0 &= a \cdot 0 + (-a \cdot 0) \\ &= (a \cdot 0 + a \cdot 0) + (-a \cdot 0) \\ &= a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) \quad \text{por asociatividad} \\ &- a \cdot 0 + 0 \\ &= a \cdot 0. \end{aligned}$$

(2) Queremos probar que $a \cdot (-b) = -(ab)$, *i.e.*, queremos probar que el inverso aditivo de ab es $a \cdot (-b)$, *i.e.*, queremos probar que $ab + a \cdot (-b) = 0$.

Para esto observamos que:

$$\begin{aligned} ab + a\cdot(-b) &= a\cdot(b+(-b)) && \text{por distributividad}\\ &= a\cdot 0 &&\\ &= 0 && \text{por la parte (1).}\end{aligned}$$

(3) Similarmente se prueba que $(-a)\cdot b = -(ab)$.

(4) Éste es un caso especial de (3) y (2) ya que

$$\begin{aligned}(-a)\cdot(-b) &= -(a\cdot(-b)) && \text{por (3)}\\ &= -(-(ab)) && \text{por (2)}\\ &= ab &&\end{aligned}$$

ya que el inverso aditivo del inverso aditivo de un elemento es el elemento dado (véase el ejercicio 6).

(5) Si $1 \in \mathbb{Z}$ es el uno, entonces,

$$\begin{aligned}(-1)\cdot a + a &= (-1)a + 1\cdot a &&\\ &= (-1+1)\cdot a && \text{(distributividad)}\\ &= 0\cdot a &&\\ &= 0 && \text{por (1)}\end{aligned}$$

y así $(-1)\cdot a = -a$. □

Ejercicio 8. Demuestre la ley de cancelación para la suma en $\mathbb{Z}$: si $a, b, c \in \mathbb{Z}$ son tales que $a + c = b + c$, entonces $a = b$.

Como uno puede esperar de nuestro conocimiento intuitivo de los enteros, $\mathbb{Z}$, y de los naturales, $\mathbb{N}$, se debe tener que $\mathbb{N} \subseteq \mathbb{Z}$. Esto lo formaliza la proposición siguiente:

Proposición III.6. *La función $\phi : \mathbb{N} \to \mathbb{Z}$ definida mediante $\phi(n) := [n + a, a]$ (para cualquier $a \in \mathbb{N}$), no depende del $a \in \mathbb{N}$, es inyectiva y preserva las operaciones de $\mathbb{N}$ y $\mathbb{Z}$, es decir:*

(1) $\phi(m + n) = \phi(m) + \phi(n)$.

(2) $\phi(mn) = \phi(m)\phi(n)$.

Nótese que en estas igualdades la suma y producto en los lados izquierdos son los de $\mathbb{N}$ y los del lado derecho son los de $\mathbb{Z}$.

Demostración. Es claro que si $a, b \in \mathbb{N}$ entonces $(n+a, a) \sim (n+b, b)$. Ahora, si $\phi(m) = \phi(n)$, entonces $[m+a, a] = [n+b, b]$ y así $(m+a, a) \sim (n+b, b)$ por lo que $(m+a)+b = a+(n+b)$, y por la ley de cancelación para la suma en $\mathbb{N}$, se sigue que $m = n$, *i.e.,* ϕ es inyectiva.

(1) $\phi(m+n) = [m+n+a, a] = [m+n+2a, 2a] = [m+a, a] + [n+a, a] = \phi(m) + \phi(n)$.

(2) $\phi(m)\phi(n) = [m+a, a][n+b, b] := [mn+x, x] = \phi(mn)$, donde $x = mb + an + 2ab \in \mathbb{N}$. □

Ejercicio 9. Demuestre que $\phi(1) = 1$, donde en el lado izquierdo el 1 es el de $\mathbb{N}$ y en el lado derecho es el de $\mathbb{Z}$. Gracias a este ejercicio no hay confusión al denotar con los mismos símbolos a los unos de $\mathbb{N}$ y de $\mathbb{Z}$.

La función inyectiva anterior $\phi : \mathbb{N} \to \mathbb{Z}$ identifica a $\mathbb{N}$ con su imagen en $\mathbb{Z}$ y así cada natural $m \in \mathbb{N}$ lo podemos ver como un entero $m = [m+a, a] \in \mathbb{Z}$.

Corolario III.7. *Si $[a, b] \in \mathbb{Z}$, consideremos los naturales $a = [a+1, 1]$ y $b = [b+1, 1]$ vistos en $\mathbb{Z}$. Entonces, en $\mathbb{Z}$ se tiene que*

$$[a, b] = a - b.$$

Demostración.

$$\begin{aligned} a - b = a + (-b) &= [a+1, 1] + (-[b+1, 1]) \\ &= [a+1, 1] + [1, b+1] \\ &= [(a+1)+1, 1+(b+1)] \\ &= [a, b]. \end{aligned}$$

□

Este corolario justifica, *a posteriori,* el pensar al entero $[a, b]$ como a la *diferencia* $a - b$, lo cual usamos como motivación para definir la relación de equivalencia que se usó para construir $\mathbb{Z}$.

III.2 El orden en $\mathbb{Z}$

La idea de un orden $x < y$ en $\mathbb{Z}$ es pensar que la diferencia $y - x$ debe ser un entero *positivo* y como ya sabemos que $\mathbb{N} \subseteq \mathbb{Z}$, podemos pensar que los números naturales son positivos y así dado un entero $[a, b] \in \mathbb{Z}$, el cual ya sabemos que es de la forma $a - b$, diremos que es *positivo* si para un representante $(a, b) \in [a, b]$ se tiene que $a > b$ en $\mathbb{N}$. Que esta definición no depende del representante elegido es el contenido del lema siguiente:

Lema III.8. *Si* $(a, b), (c, d) \in [a, b]$, *entonces* $a > b$ *en* $\mathbb{N}$ *si y sólo si* $c > d$ *en* $\mathbb{N}$.

Demostración. Observamos primero que $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. Ahora, si $a > b$ en $\mathbb{N}$, entonces existe $n \in \mathbb{N}$ tal que $a = b + n$ y substituyendo esta igualdad en $a + d = b + c$ obtenemos que $(b + n) + d = b + c$ de donde cancelando b se sigue que $c = d + n$ por lo que $c > d$. El recíproco es similar. □

Podemos entonces definir

$$\mathbb{Z}^+ := \{[a, b] \in \mathbb{Z} \ : \ \forall (a, b) \in [a, b] \ \text{ se tiene que } a > b\}$$

y a los miembros de $\mathbb{Z}^+$ los llamamos *enteros positivos.*

Proposición III.9. *El conjunto* $\mathbb{Z}^+$ *de enteros positivos satisface:*

(1) $\mathbb{Z}^+$ *es cerrado bajo sumas:* $a, b \in \mathbb{Z}^+ \Rightarrow a + b \in \mathbb{Z}^+$.

(2) $\mathbb{Z}^+$ *es cerrado bajo productos:* $a, b \in \mathbb{Z}^+ \Rightarrow ab \in \mathbb{Z}^+$.

(3) (Tricotomía): *Si* $[a, b] \in \mathbb{Z}$ *entonces una y sólo una de las posibilidades siguientes es cierta:*

(i) $[a, b] = 0$.

(ii) $[a, b] \in \mathbb{Z}^+$.

(iii) $-[a, b] \in \mathbb{Z}^+$.

Demostración. Las partes (1) y (2) las dejamos como ejercicio. Para (3), dado $[a, b] \in \mathbb{Z}$, si $(a, b) \in [a, b]$ es un representante, como $a, b \in \mathbb{N}$ entonces por la tricotomía del orden de $\mathbb{N}$ se tiene que:

(i) $a = b$ o (ii) $a > b$ o (iii) $b > a$.

En el caso (I) $[a,b] = 0 \in \mathbb{Z}$. En el caso (II) $[a,b] \in \mathbb{Z}^+$. En el caso (III) $-[a,b] = [b,a] \in \mathbb{Z}^+$. □

EJERCICIO 10. Demuestre que $\mathbb{Z}^+$ es cerrado bajo sumas y productos.

Observación. Es claro que $1 = [1+a, a] \in \mathbb{Z}^+$. Al conjunto $\mathbb{Z}^+$ lo llamamos una *clase positiva* en $\mathbb{Z}$.

Usando a la clase positiva $\mathbb{Z}^+$ de $\mathbb{Z}$ se define la *relación de orden* $<$ en $\mathbb{Z}$ como sigue: si $a, b \in \mathbb{Z}$ diremos que $a < b$ si $b - a \in \mathbb{Z}^+$. Si $a < b$ también usaremos la notación $b > a$. Nótese que $b > 0$ en $\mathbb{Z}$ quiere decir que $b \in \mathbb{Z}^+$. En particular todo natural $n \in \mathbb{N}$ es positivo y así $\mathbb{N} \subseteq \mathbb{Z}^+$.

EJERCICIO 11. Demuestre que $\mathbb{N} = \mathbb{Z}^+$.

TEOREMA III.10. *La relación $<$ en $\mathbb{Z}$ satisface las propiedades siguientes:*

(1) *Es transitiva, i.e., $a < b$ y $b < c$ implican que $a < c$.*

(2) *Es compatible con la suma: $a < b$ y $c \in \mathbb{Z} \Rightarrow a + c < b + c$.*

(3) *Es compatible con el producto:*

(I) $a < b$ y $c > 0 \Rightarrow ac < bc$.

(II) $a < b$ y $c < 0 \Rightarrow ac > bc$.

Demostración. (1) $a < b$ y $b < c$ quieren decir que $b - a \in \mathbb{Z}^+$ y $c - b \in \mathbb{Z}^+$, y como $\mathbb{Z}^+$ es cerrado bajo sumas, entonces $c - a = (b - a) + (c - b) \in \mathbb{Z}^+$, es decir, $a < c$.

(2) $a < b$ quiere decir que $b - a \in \mathbb{Z}^+$ y así

$$(b + c) - (a + c) = b - a \in \mathbb{Z}^+$$

por lo que $a + c < b + c$.

(3) (I) $a < b$ quiere decir que $b - a \in \mathbb{Z}^+$ y $c > 0$ quiere decir que $c \in \mathbb{Z}^+$, y como $\mathbb{Z}^+$ es cerrado bajo productos, entonces $(b - a)c \in \mathbb{Z}^+$, es decir, $bc - ac \in \mathbb{Z}^+$, *i.e.*, $ac < bc$.

(II) $a < b$ quiere decir que $b - a \in \mathbb{Z}^+$ y $c < 0$ implica que $-c \in \mathbb{Z}^+$. Se sigue que $(b - a)(-c) \in \mathbb{Z}^+$, es decir, $ac - bc \in \mathbb{Z}^+$, *i.e.*, $ac > bc$. □

EJERCICIO 12. Demuestre que si $a < b$ y $c < d$ en $\mathbb{Z}$, entonces $a + c < b + d$.

Dados dos enteros $a, b \in \mathbb{Z}$, diremos que $a \leq b$ si $a < b$ o $a = b$.

EJERCICIO 13. Demuestre que la relación $\leq$ es una relación reflexiva, antisimétrica y transitiva en $\mathbb{Z}$.

EJERCICIO 14. Si $a < b$ y $b \leq c$, demuestre que $a < c$.

EJERCICIO 15. Demuestre que si $a \in \mathbb{Z}$ y $a \neq 0$, entonces $a^2 > 0$.

EJERCICIO 16. Demuestre que si $a < b$ en $\mathbb{Z}$, entonces $-a > -b$.

El valor absoluto de un entero. Si $a \in \mathbb{Z}$, se define su valor absoluto, denotado $|a|$, como:

$$|a| := \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0. \end{cases}$$

EJERCICIO 17. Si $a \in \mathbb{Z}$, demuestre que $|a| = |-a|$.

EJERCICIO 18. Demuestre que el valor absoluto es una función $|\ \ | : \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ que satisface las propiedades siguientes:

(I) $\forall a \in \mathbb{Z}$ se tiene que $|a| \geq 0$ y más aún, $|a| = 0 \Leftrightarrow a = 0$.

(II) $\forall a \in \mathbb{Z}$ se tiene que $\pm a \leq |a|$.

(III) $|ab| = |a||b|$ $\forall a, b \in \mathbb{Z}$.

(IV) $|a + b| \leq |a| + |b|$ $\forall a, b \in \mathbb{Z}$ (desigualdad del triángulo).

Si A es un anillo conmutativo con 1, dado un elemento $u \in A$, un *inverso multiplicativo* de u es otro elemento $v \in A$ tal que $uv = 1$. Por ejemplo, para el $1 \in A$ un inverso multiplicativo es él mismo ya que $1 \cdot 1 = 1$. Otro ejemplo es el $-1 \in A$ cuyo inverso multiplicativo es él mismo ya que $(-1)(-1) = 1$ por (III.7)(4). Por supuesto que, en general, un inverso multiplicativo de un elemento $u \in A$ puede ser distinto de u. Esto lo veremos en los ejemplos de la subsección siguiente.

EJERCICIO 19. Si A es un anillo conmutativo con uno, demuestre que el inverso multiplicativo de un elemento $u \in A$ es único. Denotaremos al inverso multiplicativo de u con u^{-1}.

EJERCICIO 20. Si A es un anillo conmutativo con uno y el elemento $u \in A$ tiene inverso multiplicativo, demuestre que $(u^{-1})^{-1} = u$.

EJERCICIO 21. Use el ejercicio 15 para demostrar que si $a \in \mathbb{Z}$ y $a > 1$, entonces a no tiene inverso multiplicativo en $\mathbb{Z}$.

EJERCICIO 22. Similarmente, demuestre que si $a \in \mathbb{Z}$ y $a < -1$, entonces a no tiene inverso multiplicativo en $\mathbb{Z}$.

EJERCICIO 23. Concluya de los dos ejercicios anteriores que los únicos elementos de $\mathbb{Z}$ que tienen inverso multiplicativo son 1 y -1.

EJERCICIO 24. Si A es un anillo conmutativo con 1, y $u, v \in A$ tienen inverso multiplicativo, entonces $uv \in A$ también tiene inverso multiplicativo.

III.3 DOMINIOS ENTEROS

A continuación probaremos una propiedad del anillo $\mathbb{Z}$ que no se puede deducir formalmente de las propiedades de anillo de $\mathbb{Z}$, a saber, que en $\mathbb{Z}$ si se tienen dos elementos distintos de cero su producto debe ser también diferente de cero. Para apreciar esta propiedad de $\mathbb{Z}$ conviene mostrar algunos anillos conmutativos con uno donde esta propiedad es falsa.

Ejemplo 1. Considere el conjunto $A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ para el cual los símbolos $\overline{x}$ los sumamos y multiplicamos de acuerdo con las tablas siguientes, donde en el primer renglón y primera columna se listan los elementos del conjunto A, y si $\overline{a}, \overline{b} \in A$, para obtener la suma $\overline{a} + \overline{b}$, localizamos a $\overline{a}$ en la primera columna y a $\overline{b}$ en el primer renglón, y la suma $\overline{a} + \overline{b}$ es el elemento dado en la casilla donde se intersectan los lugares de $\overline{a}$ y $\overline{b}$:

$+$			$\overline{b}$	
$\overline{a}$			$\overline{a}+\overline{b}$	

similarmente para el producto $\overline{a} \cdot \overline{b}$.

Las tablas de suma y producto del conjunto $A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ de este ejemplo son:

SUMA:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

PRODUCTO:

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

EJERCICIO 25. Compruebe que A con las operaciones anteriores es un anillo conmutativo con uno.

Notamos ahora que en este ejemplo el elemento $\overline{2} \neq \overline{0}$ y sin embargo en la tabla de multiplicación de este anillo se tiene que $\overline{2} \cdot \overline{2} = \overline{0}$.

A un elemento a (como el $\overline{2}$ del ejemplo anterior) que es diferente de cero y para el cual existe otro elemento distinto de cero b en A tal que $ab = 0$ se le llama un *divisor propio de cero* del anillo A. Así, lo que queremos probar es que en $\mathbb{Z}$ no hay divisores propios de cero. Un anillo conmutativo con uno que no tiene divisores propios de cero se llama un *dominio entero*.

EJERCICIO 26. Encuentre los elementos del anillo anterior que tienen inverso multiplicativo.

Ejemplo 2. Considere el conjunto $A = \{\overline{0}, \overline{1}, \overline{2}\}$ donde los símbolos $\overline{x}$ los sumamos y multiplicamos de acuerdo con las tablas siguientes:

SUMA:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

PRODUCTO:

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Este anillo es un dominio entero, como se puede comprobar fácilmente mirando a su tabla de multiplicar: en efecto, en esta tabla los únicos ceros aparecen cuando uno de los factores es cero, es decir, en la columna y renglón del cero, a diferencia del ejemplo anterior donde aparecía un cero fuera de la columna y renglón del cero.

EJERCICIO 27. Encuentre los elementos del anillo anterior que tienen inverso multiplicativo.

EJERCICIO 28. Considere el conjunto $A = \{\overline{0}, \overline{1}\}$ donde los símbolos $\overline{x}$ los sumamos y multiplicamos de acuerdo con las tablas siguientes:

SUMA:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

PRODUCTO:

$\bullet$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Muestre que es un dominio entero.

EJERCICIO 29. Encuentre los elementos del anillo anterior que tienen inverso multiplicativo.

EJERCICIO 30. Considere el conjunto $A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ donde los símbolos $\overline{x}$ los sumamos y multiplicamos de acuerdo con las tablas siguientes:

SUMA:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

PRODUCTO:

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Muestre que no es un dominio entero.

EJERCICIO 31. Encuentre los elementos del anillo anterior que tienen inverso multiplicativo.

Los ejemplos anteriores muestran que la propiedad de ser dominio entero es bastante especial y no la tienen todos los anillos conmutativos con uno. El hecho de que $\mathbb{Z}$ sea un dominio entero debe entonces probarse usando su definición como un conjunto cociente de una cierta relación de equivalencia:

TEOREMA III.11. *El anillo $\mathbb{Z}$ es un dominio entero.*

Demostración. Sean $\alpha = [a, b]$ y $\beta = [c, d]$ en $\mathbb{Z}$ tales que $\alpha\beta = 0$. Mostraremos que $\alpha = 0$ o $\beta = 0$. Si $\alpha = 0$, no hay nada que probar. Supongamos entonces que $\alpha \neq 0$ y observemos que de la igualdad

$$\alpha\beta = [a, b][c, d] = [ac + bd, ad + bc] = 0$$

se sigue que $ac + bd = ad + bc$ por definición del 0 de $\mathbb{Z}$. Ahora, como $\alpha \neq 0$, entonces $a \neq b$ en $\mathbb{N}$, y por tricotomía se sigue que $a < b$ o $b < a$. En el primer caso se tiene que $b = a + n$, lo que substituido en la igualdad $ac + bd = ad + bc$ nos da $ac + (a + n)d = ad + (a + n)c$, es decir, $ac + ad + nd = ad + ac + nc$ de donde, por la ley de cancelación para la suma en $\mathbb{N}$, se sigue que $nd = nc$ que, por la ley de cancelación para el producto, implica que $d = c$, *i.e.*, $\beta = 0$. El caso $b < a$ es similar. □

Como una consecuencia de que $\mathbb{Z}$ es un dominio entero se tiene la ley de cancelación para el producto en $\mathbb{Z}$:

Corolario III.12 (Ley de cancelación para el producto en $\mathbb{Z}$). *Si a, b, c en $\mathbb{Z}$ son tales que $ac = bc$ con $c \neq 0$, entonces $a = b$.*

Demostración. $ac = bc$ implica que $(a - b)c = 0$ con $c \neq 0$, y como $\mathbb{Z}$ es dominio entero, se debe entonces tener que $a - b = 0$, *i.e.*, $a = b$. □

El corolario anterior de hecho nos dice que la propiedad de ser dominio entero implica la ley de cancelación para el producto.

Ejercicio 32. Demuestre que la ley de cancelación para el producto en $\mathbb{Z}$ implica la propiedad de ser dominio entero.

Así, de alguna forma podríamos haber probado que $\mathbb{Z}$ satisface la ley de cancelación para el producto y de ahí deducir que $\mathbb{Z}$ es un dominio entero. En otras palabras, la propiedad de ser dominio entero es equivalente a la ley de cancelación para el producto.

III.4 Divisibilidad en $\mathbb{Z}$

Dados enteros a, b con $b \neq 0$, para comenzar mostraremos que podemos dividir a entre b obteniendo un cociente q y un residuo r cuando la división termine, es decir, cuando r sea menor que b. Usaremos la notación $a = bq + r$

para lo anterior. Así, como a, b con $b \neq 0$ están dados, lo que debemos hacer es mostrar la existencia de los enteros $q, r \in \mathbb{Z}$ tales que $a = bq + r$ y $0 \leq r < |b|$:

TEOREMA III.13 (Algoritmo de la división). *Si a, b son enteros con $b \neq 0$, entonces existen enteros q, r tales que*

$$a = bq + r \quad \text{y} \quad 0 \leq r < |b|.$$

Demostración. Sea $M = \{a - bt \in \mathbb{Z} \,:\, t \in \mathbb{Z}\}$ y observemos que al variar t, no importa cuáles sean los enteros a, b siempre hay enteros ≥ 0 de la forma $a - bt$ por lo que $M \cap (\mathbb{N} \cup \{0\}) \neq \emptyset$. Por el principio del buen orden[1] existe un elemento menor ≥ 0 en M. Denotemos por $r = a - bq$ a este elemento ≥ 0 menor de M. Entonces $a = bq + r$ y sólo falta probar que $r < |b|$. Para esto, supongamos primero que $b > 0$ de tal forma que $|b| = b$. Si sucediera que $r \geq b$, entonces:

$$a - b(q+1) = (a - bq) - b = r - b \geq 0 \tag{1}$$

y por otra parte

$$a - b(q+1) = (a - bq) - b < a - bq = r, \tag{2}$$

es decir, (1) y (2) contradicen la minimalidad de r. Se sigue que $r < b$ como se quería.

Para el caso $b < 0$ restante, observamos que $-b > 0$ por lo que aplicando el caso anterior se tiene que $a = (-b)(-q) + r$ con $0 \leq r < -b = |b|$. □

¿Cómo podemos calcular, en la práctica, el cociente q y el residuo r de dividir un entero a entre otro entero $b \neq 0$? Para comenzar, supongamos que $b > 0$; observemos que, al dividir la igualdad $a = bq + r$ entre $b > 0$ obtenemos

$$\frac{a}{b} = q + \frac{r}{b} \quad \text{con} \quad 0 \leq \frac{r}{b} < 1$$

por lo que

$$q = \text{parte entera de } \frac{a}{b} = \text{mayor entero} \leq \frac{a}{b} = \left[\frac{a}{b}\right],$$

[1] El principio del buen orden de $\mathbb{N}$ se extiende en forma obvia a los enteros ≥ 0.

donde la fracción a/b se puede obtener con una calculadora. Esto facilita el cálculo de q y el residuo r se calcula después mediante $r = a - bq$.

EJERCICIO 33. ¿Qué sucede si $b < 0$?, es decir, ¿cómo se calcula q en este caso?

Divisibilidad. Dados dos enteros a, b con $a \neq 0$, al dividir b entre a puede suceder que el residuo sea 0, es decir, que se tenga que $b = aq$ con $r = 0$ en el algoritmo de la división anterior. En este caso diremos que a *divide* a b y lo denotamos mediante $a|b$. Algunas veces también diremos que a es un *divisor* o *factor* de b, o que b es un *múltiplo* de a. En el caso cuando a no divide a b lo denotamos $a \nmid b$. Hemos así definido una relación en el anillo $\mathbb{Z}$ y las primeras propiedades de esta relación son las siguientes:

PROPOSICIÓN III.14. (1) *Para toda $a \neq 0$ en $\mathbb{Z}$ se tiene que $a|a$.*

(2) *Si $a|b$ y $b|c$ entonces $a|c$. (Transitividad.)*

(3) $1|a$ *para toda* $a \in \mathbb{Z}$.

(4) *Si $a|b$ y $a|c$ entonces $a|b + c$.*

(5) *Si $a|b$ y $c \in \mathbb{Z}$ es arbitrario, entonces $a|bc$.*

(6) *Si $a|b$ y $a|c$ entonces $a|bs + ct$ para cualesquiera $s, t \in \mathbb{Z}$.*

NOTA: Si b, c son dos enteros fijos, a cualquier expresión de la forma $bs + ct$ con $s, t \in \mathbb{Z}$, se le llama una *combinación lineal* de b y c.

Demostración. Todas estas propiedades son directas de la definición. Por ejemplo, para (1), $a = a \cdot 1$. Para (2), como $a|b$ y $b|c$ entonces $b = aq$ y $c = br$ por lo que $c = br = (aq)r = a(qr)$ y así $a|c$. Para (3), $a = 1 \cdot a$. Para (4), como $b = aq$ y $c = ar$, entonces $b + c = a(q + r)$. Para (5), como $b = aq$ entonces $bc = a(qc)$ por lo que $a|bc$. La parte (6) se sigue de (4) y (5). Nótese que si hubiéramos probado primero (6) entonces (4) y (5) son casos particulares de (6). □

EJERCICIO 34. Demuestre que si $a|b$ entonces $a| - b$, $-a|b$ y $-a| - b$.

EJERCICIO 35. Demuestre que si a divide a cualquier combinación lineal $bs + ct$ de b y c, entonces $a|b$ y $a|c$.

EJERCICIO 36. Demuestre que si $a|1$ entonces $a = \pm 1$.

EJERCICIO 37. Demuestre que si $a|b$ y $b|a$, entonces $a = \pm b$.

EJERCICIO 38. Demuestre que si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$.

EJERCICIO 39. Use inducción (sobre n) para probar que si $a|b_1, \ldots, a|b_n$ y $r_1, \ldots, r_n$ son enteros arbitrarios, entonces $a|(r_1 b_1 + \cdots + r_n b_n)$.

El máximo común divisor. Dados dos enteros fijos a, b, con alguno de ellos $\neq 0$, podemos considerar el conjunto de divisores comunes a ambos enteros. Por el ejercicio (38), si d es un divisor común de a, b, y si, por ejemplo $a \neq 0$, entonces $|d| \leq |a|$, y como $|a|$ está fijo, entonces existe un mayor divisor común d de a y b. Este d se llamará un *máximo común divisor* de a y b. Sin embargo, nosotros adoptaremos otra definición de un máximo común divisor de a y b que es equivalente a la anterior pero es más manejable. La definición que usaremos es la siguiente: dados dos enteros a, b, con alguno de ellos $\neq 0$, un *máximo común divisor* de a y b es un entero g tal que:

(I) $g|a$ y $g|b$. (Es decir, g es divisor común.)

(II) Para cualquier $d \in \mathbb{Z}$ tal que $d|a$ y $d|b$ se tiene que $d|g$. (En este sentido d es más chico que g ya que el ejercicio (38) nos dice que $|d| \leq |g|$.)

A continuación mostraremos que dados cualesquiera dos enteros a, b, con alguno de ellos $\neq 0$, un máximo común divisor de a y b existe y de hecho es único salvo el signo. Comenzamos mostrando la unicidad:

LEMA III.15. *Sean a, b dos enteros con alguno de ellos $\neq 0$ y supongamos que g_1 y g_2 son dos máximos comunes divisores de a y b. Entonces, $g_1 = \pm g_2$.*

Demostración. Como $g_2|a$ y $g_2|b$ y como g_1 es máximo común divisor de a y b entonces $g_1|g_2$ por la propiedad (II). Similarmente, cambiando los papeles de g_1 y g_2 se sigue que $g_2|g_1$. El ejercicio (37) nos dice entonces que $g_1 = \pm g_2$. □

Gracias a este resultado, dados dos enteros a, b, con alguno de ellos $\neq 0$, si un máximo común divisor de a, b existe, siempre lo podemos elegir positivo y a esta elección la llamaremos *el máximo común divisor de a, b* y lo denotaremos mediante $g = \text{mcd}(a, b)$. La existencia del máximo común divisor de cualquier par de enteros dados la garantiza el teorema siguiente:

TEOREMA III.16. *Sean $a, b \in \mathbb{Z}$ con alguno de ellos $\neq 0$. Entonces, el máximo común divisor g de a, b existe y de hecho g es la menor combinación lineal positiva de a, b.*

Demostración. Como $a \neq 0$ o $b \neq 0$; entonces, el conjunto de combinaciones lineales distintas de cero de a, b:

$$M = \{as + bt \ : \ s, t \in \mathbb{Z}\} - \{0\}$$

es no vacío y, de hecho, eligiendo s, t adecuadamente se tiene que existen combinaciones lineales $as + bt > 0$ por lo que $M \cap \mathbb{N} \neq \emptyset$. Por el principio de buen orden existe un elemento menor g en $M \cap \mathbb{N}$, *i.e.*, g es la menor combinación lineal positiva de a, b, digamos $g = as_0 + bt_0$. Mostraremos ahora que $g|a$ y $g|b$. Basta mostrar que $g|a$ y para esto supongamos que $g \nmid a$. Entonces $g \nmid -a$ y por lo tanto $g \nmid |a|$ por lo que podemos suponer, sin perder generalidad, que $a > 0$ y como $g \nmid a$ entonces $a = gq + r$ con $0 < r < g$. Observamos ahora que $r = a - gq \in M$ ya que

$$r = a - gq = a - (as_0 + bt_0)q = a(1 - s_0 q) + b(-t_0 q),$$

i.e., r es combinación lineal de a, b y como $r > 0$ entonces r es una combinación lineal positiva de a, b, lo cual contradice la minimalidad de g ya que $r < g$. Se debe entonces tener que $g|a$ y similarmente $g|b$.

Finalmente, si $d \in \mathbb{Z}$ es tal que $d|a$ y $d|b$ entonces d divide a cualquier combinación lineal de a y b, en particular $d|g$. Hemos así probado que $g = \text{mcd}(a, b)$. □

EJERCICIO 40. Si $a \neq 0$, demuestre que $\text{mcd}(a, 0) = |a|$.

EJERCICIO 41. Demuestre que $\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$.

EJERCICIO 42. Sean $a, b \in \mathbb{Z}$ y $d = \text{mcd}(a, b)$. Si $a = da'$ y $b = db'$, demuestre que $\text{mcd}(a', b') = 1$. Cuando dos enteros tienen mcd igual a 1, decimos que estos enteros son *coprimos* o *primos relativos*. Así, en este ejercicio se pide probar que a', b' son coprimos.

EJERCICIO 43. Si a, b son coprimos y $c|a$, demuestre que b y c son coprimos también.

EJERCICIO 44. Demuestre que para todo $r \in \mathbb{Z}$ se tiene que $\text{mcd}(a, b+ar) = \text{mcd}(a, b)$.

EJERCICIO 45. Demuestre que para todo $c \geq 1$ se tiene que $\text{mcd}(ca, cb) = c \cdot \text{mcd}(a, b)$.

EJERCICIO 46. Demuestre que si m es combinación lineal de a y b, entonces para todo $r \in \mathbb{Z}$ se tiene que rm también es combinación lineal de a y b.

EJERCICIO 47. Si d es combinación lineal de a, b y b es combinación lineal de a, c, demuestre que d es combinación lineal de a y c.

EJERCICIO 48. Los ejemplos siguientes ilustran el concepto de combinación lineal de dos enteros:

(I) Escriba a 24 como combinación lineal de 3 y 6.

(II) Muestre que 52 no es combinación lineal de 20 y 15.

(III) Si m es impar, demuestre que no es combinación lineal de 198 y 290.

(IV) Si $m = 3t + 1$ con $t \in \mathbb{Z}$, demuestre que m no es combinación lineal de 45 y 1251.

El algoritmo de Euclides. Dados dos números enteros a, b se tiene la pregunta natural de cómo se puede calcular, en forma eficiente, el $\text{mcd}(a, b)$. Una primera idea, ineficiente, es listar todos los divisores positivos de a y luego los de b. De estas listas se elige entonces el mayor divisor positivo común. El método siguiente que, de hecho, es un algoritmo, se debe a Euclides[2] y es bastante más eficiente que el método anterior, como el lector puede confirmar con algún ejemplo. El algoritmo de Euclides para calcular el $\text{mcd}(a, b)$ de dos enteros a, b dados es como sigue: para comenzar podemos suponer que a y b son ambos positivos por el ejercicio (41). Supongamos además que $a \geq b$. Entonces, dividiendo a entre b escribamos:

$$a = bq_1 + r_1 \qquad \text{con } 0 \leq r_1 < b. \tag{1}$$

Si $r_1 = 0$, entonces $a = bq_1$ por lo que $b|a$ y así $\text{mcd}(a, b) = b$. Si $r_1 > 0$ entonces dividimos b entre r_1:

$$b = r_1 q_2 + r_2 \qquad \text{con } 0 \leq r_2 < r_1. \tag{2}$$

[2]Véanse las proposiciones 1 y 2 del libro 7 de los *Elementos* de Euclides.

Si $r_2 = 0$, mostraremos que r_1 es $\mathrm{mcd}(a, b)$. En efecto, como $r_2 = 0$, de (2) se tiene que $b = r_1 q_2$ por lo que $r_1 | b$. Ahora, por (1), $a = bq_1 + r_1$ y como $r_1 | b$ entonces $r_1 | bq_1 + r_1$ por lo que $r_1 | a$. Se sigue que $r_1 | a$ y $r_1 | b$. Supongamos ahora que $d | a$ y $d | b$; entonces $d | a - bq_1 - r_1$, *i.e.*, $d | r_1$. Hemos así mostrado que $r_1 = \mathrm{mcd}(a, b)$. Si $r_2 > 0$, entonces dividimos r_1 entre r_2:

$$r_1 = r_2 q_3 + r_3 \qquad \text{con } 0 \leq r_3 < r_2. \tag{3}$$

Se tienen de nuevo dos casos: si $r_3 = 0$, mostraremos que $r_2 = \mathrm{mcd}(a, b)$. En efecto, como $r_3 = 0$ entonces $r_2 | r_1$ y la ecuación (2) implica que $r_2 | b$ y así, usando la ecuación (1) se sigue que $r_2 | a$. Hemos así mostrado que $r_2 | a$ y $r_2 | b$. Supongamos ahora que $d | a$ y $d | b$. Entonces la ecuación (1) implica que $d | a - bq_1 = r_1$ y usando la ecuación (2) se sigue que $d | r_2$ y por lo tanto $r_2 = \mathrm{mcd}(a, b)$. Si $r_3 > 0$, dividimos r_2 entre r_3:

$$r_2 = r_3 q_4 + r_4 \qquad \text{con } 0 \leq r_4 < r_3 \tag{4}$$

y procedemos como antes, etc. Este proceso tiene que terminar ya que se van obteniendo enteros positivos:

$$0 \leq r_{n+1} < r_n < \cdots < r_3 < r_2 < r_1 < b$$

en las igualdades:

$$\begin{aligned}
a &= bq_1 + r_1 && \text{con} && 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2 && \text{con} && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && \text{con} && 0 \leq r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4 && \text{con} && 0 \leq r_4 < r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} && \text{con} && 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n && \text{con} && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 && \text{con} && r_{n+1} = 0
\end{aligned}$$

y el resultado neto es:

PROPOSICIÓN III.17 (Algoritmo de Euclides). *Si $a, b \in \mathbb{Z}$, en las igualdades anteriores el último residuo distinto de cero, r_n, es el* mcd *de a y b. Más aún, despejando a r_n de la igualdad correspondiente y substituyendo en las anteriores, se obtiene a r_n como combinación lineal de a y b.*

Demostración. La última igualdad nos dice que $r_n | r_{n-1}$ por lo que la penúltima igualdad implica que $r_n | r_{n-2}$. Subiendo en la lista de igualdades anterior se sigue que $r_n | r_j$ para todo j y por lo tanto $r_n | a$ y $r_n | b$. Supongamos ahora que $d|a$ y $d|b$. La primera igualdad de la lista anterior implica que $d|r_1$ por lo que la segunda igualdad implica que $d|r_2$. Descendiendo por la lista anterior se sigue que $d|r_j$ para toda j, en particular $d|r_n$. Hemos así mostrado que $r_n = \text{mcd}(a, b)$.

Finalmente, despejando a r_n de la penúltima igualdad y substituyendo el valor despejado de r_{n-1} de la igualdad previa en la fórmula para r_n, obtenemos a r_n como combinación lineal de los residuos anteriores. Se procede recursivamente como antes para al final expresar a r_n como combinación lineal de a y b. □

Ejemplo 3. Usando el algoritmo de Euclides, calcular $\text{mcd}(14, 400)$ y expresarlo como la combinación lineal correspondiente:

$$\begin{aligned} 400 &= (14)(28) + 8 \\ 14 &= (8)(1) + 6 \\ 8 &= (6)(1) + 2 \\ 6 &= (2)(3). \end{aligned}$$

Como el último residuo distinto de 0 es 2, se tiene que $\text{mcd}(14, 400) = 2$. Finalmente, despejando de las igualdades anteriores:

$$\begin{aligned} 2 &= 8 - (6)(1) \\ &= 8 - (14 - (8)(1))(1) \\ &= (8 + 8) - 14 = 8(2) - 14 \\ &= (400 - 14(28))2 - 14 = 400(2) - 14(56) - 14 \\ &= 400(2) + 14(-57), \end{aligned}$$

y ésta es la combinación lineal buscada.

Nota. En los despejes anteriores las multiplicaciones van quedando indicadas para al final poder factorizar en cada sumando a los números $a = 400$ y $b = 14$ conservando su signo.

EJERCICIO 49. Usando el algoritmo de Euclides calcule los siguientes máximos comunes divisores:

(I) $\mathrm{mcd}(2947, 3997)$.

(II) $\mathrm{mcd}(329, 1005)$.

(III) $\mathrm{mcd}(1302, 1224)$.

(IV) $\mathrm{mcd}(7469, 2464)$.

(V) $\mathrm{mcd}(2689, 4001)$.

(VI) $\mathrm{mcd}(1109, 4999)$.

(VII) $\mathrm{mcd}(1819, 3587)$.

EJERCICIO 50. Exprese los $\mathrm{mcd}(a, b)$ del ejercicio anterior como combinación lineal de los enteros a, b dados.

III.5 El teorema fundamental de la aritmética

Dados dos enteros a, b, recordemos que se dice que son *coprimos* si $\mathrm{mcd}(a, b) = 1$. El resultado siguiente, atribuido algunas veces a Euclides,[3] es de fundamental importancia para la aritmética:

TEOREMA III.18 (Primer teorema de Euclides). *Si* $a|bc$ *y* $\mathrm{mcd}(a, b) = 1$, *entonces* $a|c$.

Demostración. Como $1 = \mathrm{mcd}(a, b)$, entonces 1 es combinación lineal de a y b, digamos $1 = as + bt$. Multiplicando esta igualdad por c queda:

$$c = c \cdot 1 = acs + bct$$

donde $a|acs$ y $a|bct$ ya que $a|bc$. Se sigue que $a|acs + bct = c$, *i.e.*, $a|c$ como se quería. □

En este teorema es importante observar que la condición $\mathrm{mcd}(a, b) = 1$ es necesaria ya que sin esta condición puede suceder que $a|bc$ y sin embargo $a \nmid b$ y $a \nmid c$. Por ejemplo, $6|(2)(3)$ pero $6 \nmid 2$ y $6 \nmid 3$.

EJERCICIO 51. Si $d|a$, $d|bc$ y $\mathrm{mcd}(a, b) = 1$, demuestre que $d|c$.

[3]Véase la proposición 30 del libro 7 de los *Elementos* de Euclides.

EJERCICIO 52. Si a, b son coprimos, demuestre que para toda $c \in \mathbb{Z}$ se tiene que $\text{mcd}(a, bc) = \text{mcd}(a, c)$.

EJERCICIO 53. Si $\text{mcd}(a, m) = 1 = \text{mcd}(b, m)$, demuestre que $\text{mcd}(ab, m) = 1$.

EJERCICIO 54. Si $\text{mcd}(a, b) = 1$, $a|c$ y $b|c$, demuestre que $ab|c$.

Un entero p se dice que es *primo* si $p \neq 0, \pm 1$ y si sus únicos divisores son ± 1 y $\pm p$. Es tradicional considerar sólo a los primos positivos, ya que si p es primo entonces $-p$ también es primo. Cuando dos enteros difieren sólo por el signo, decimos que son *asociados*. Así, cualquier primo es asociado de un primo positivo. Un entero a que no sea 0 o ± 1 y que no sea primo se llama *compuesto*.

Ejemplo 4. Los enteros siguientes son primos: 2,3,5,7,11,13,17,19,23,29,31,37.

Una primera pregunta que se ocurre es: ¿cómo encontrar los primos en la lista de todos los enteros positivos? El método siguiente se debe a Eratóstenes y es como sigue: para hallar los primos en una lista de enteros positivos del 1 al n, primero listamos los enteros positivos entre 1 y n; después, como 1 no es primo por definición, entonces lo tachamos de la lista:

$$\not{1}, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots, n.$$

El primer entero no tachado después del 1, es primo; en este caso es el 2. Después tachamos a todos los múltiplos de 2, con excepción del 2, en la lista anterior:

$$\not{1}, 2, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11, \ldots, n.$$

El primer entero no tachado es primo; en este caso es el 3. Después tachamos a todos los múltiplos de 3, exceptuando al 3:

$$\not{1}, 2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \ldots, n.$$

El primer entero no tachado es primo; en este caso es el 5. Después tachamos a todos los múltiplos de 5, exceptuando al 5 y el primer entero no tachado será primo, en este caso el 7. Por ejemplo si quisiéramos todos los primos menores que $n = 20$, la lista anterior sería:

$$\not{1}, 2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20},$$

por lo que $2, 3, 5, 7, 11, 13, 17, 19$ son todos los primos menores que 20. El método anterior se llama la *criba de Eratóstenes* ya que funciona como una coladera o *criba* al filtrar a los primos de la lista del 1 al n. El ejercicio (58) nos dice que para encontrar la lista de primos del 1 al n basta ir tachando múltiplos de primos, hasta que lleguemos al primo p más cercano a $\sqrt{n}$.

Nuestro objetivo ahora es probar que todo entero $a > 1$ se puede factorizar, en forma esencialmente única, como producto de primos, de tal forma que los enteros primos son como los ladrillos a partir de los cuales se construye a todos los otros enteros. La parte importante de este resultado es la unicidad de la factorización y para probarlo necesitaremos una consecuencia del primer teorema de Euclides y también del cálculo siguiente:

LEMA III.19. *Si p es primo, entonces* $\mcd(p, a) = \begin{cases} 1 & \text{si } p \nmid a \\ p & \text{si } p|a. \end{cases}$

Demostración. Los únicos divisores positivos de p son 1 y p, por lo que $\mcd(p, a)$ es 1 o p. Se sigue que: $p \nmid a \iff \mcd(p, a) = 1$ y $p|a \iff \mcd(p, a) = p$. □

Usando este lema, junto con el primer teorema de Euclides,[4] se tiene la consecuencia siguiente:

COROLARIO III.20. *Si p es primo y $p|ab$, entonces $p|a$ o $p|b$.*

Demostración. Si $p|a$ no hay nada que probar. Supongamos entonces que $p \nmid a$; entonces, por el lema anterior $\mcd(p, a) = 1$ y como $p|ab$, por el teorema de Euclides se sigue que $p|b$. □

EJERCICIO 55. Si p es primo y $p|a_1 \cdots a_n$, demuestre (por inducción sobre n) que existe un índice j entre 1 y n tal que $p|a_j$.

EJERCICIO 56. Si p es primo y $p|a^n$ para $n \in \mathbb{N}$, demuestre que $p|a$.

EJERCICIO 57. Dé ejemplos donde las afirmaciones de los dos ejercicios anteriores sean falsas cuando p no es primo.

EJERCICIO 58. Si $m > 2$ no es primo, demuestre que existe un primo p que divide a m y además $p \leq \sqrt{m}$.

[4]De hecho, este corolario es la proposición 30 del libro 7 de los *Elementos* de Euclides.

TEOREMA III.21 (Teorema fundamental de la aritmética). *Todo entero a que no sea 0 o ± 1 se puede factorizar de la forma:*

$$a = p_1 p_2 \cdots p_r$$

con los p_i primos y esta factorización de a es esencialmente única, es decir, si

$$a = q_1 q_2 \cdots q_s$$

es otra factorización de a con los q_j primos, entonces $r = s$ y existe una biyección $\sigma : \mathbb{I}_r \to \mathbb{I}_r$ tal que $p_i = q_{\sigma(i)}$, donde $\mathbb{I}_r = \{1, 2, 3, \ldots, r\} \subseteq \mathbb{N}$.

Demostración. (Existencia de la factorización.) Como a no es igual a 0 o ± 1, entonces $|a| > 1$ por lo que $a > 1$ o $a < -1$. Si $a < -1$, entonces $-a > 1$ y si factorizamos a $-a$ como producto de primos, digamos $-a = p_1 p_2 \cdots p_r$, entonces $a = (-p_1)p_2 \cdots p_r$ es la factorización deseada. Podemos entonces suponer que $a > 1$ y entonces haremos inducción sobre el entero positivo a. Si a es primo, digamos $a = p$, entonces ésta es la factorización deseada. Si a no es primo, entonces a es compuesto y lo podemos escribir como $a = bc$ con $1 < b < a$ y $1 < c < a$. Por hipótesis de inducción, como b y c son menores que a, éstos se pueden factorizar como producto de primos, digamos:

$$b = p_1 \cdots p_m \qquad \text{y} \qquad c = q_1 \cdots q_n$$

con los p_i y q_j primos. Juntando estas dos factorizaciones se tiene que:

$$a = bc = p_1 \cdots p_m q_1 \cdots q_n$$

es una factorización de a en primos.

Unicidad de la factorización: supongamos que

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

son dos factorizaciones de a con los p_i y q_j primos. Sin perder generalidad podemos suponer que $r \leq s$. Entonces, la igualdad

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \tag{1}$$

implica que $p_1 | q_1 q_2 \cdots q_s$ y como p_1 es primo, por el corolario al primer teorema de Euclides (véase el ejercicio 55) se sigue que p_1 divide a algún q_j. Reordenando los primos q_j, si hiciera falta, podemos suponer que $q_j = q_1$, por lo que $p_1 | q_1$ y como ambos son primos esto implica que $p_1 = q_1$. Así, podemos cancelar a $p_1 = q_1$ de la igualdad (1) para obtener:

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s \tag{2}$$

y esta igualdad implica que p_2 divide a $q_2 q_3 \cdots q_s$ y de nuevo usando el mismo argumento que arriba se sigue que $p_2 = q_j$ para $2 \leq j \leq s$, y reordenando de nuevo podemos suponer que $p_2 = q_2$. Cancelamos este factor de (2) para obtener

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s. \tag{3}$$

Procedemos recursivamente de esta forma hasta cancelar a todos los primos p_i (recuerde que estamos suponiendo que $r \leq s$) para que al final quede:

$$1 = q_{r+1} \cdots q_s$$

lo cual es imposible a menos que al mismo tiempo se hayan cancelado todos los primos q_j, es decir, $r = s$. Nótese que en el procedimiento anterior en cada paso se hacía una reordenación de los primos q_j. Esto nos da la biyección deseada. □

Si $a > 1$ es un entero y se tiene la factorización provista por el teorema anterior:

$$a = p_1 p_2 \cdots p_r$$

entonces juntando los primos iguales podemos escribir esta factorización de la forma:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

con los p_j primos distintos y los exponentes $e_j \geq 1$.

Ejemplo 5. Factorice el entero $a = 360$. Usando la tabla siguiente obtenemos los factores primos de 360:

360	2
180	2
90	2
45	3
15	3
5	5
1	

Por lo que $360 = 2^3 \cdot 3^2 \cdot 5$.

La factorización anterior nos da un método para calcular el mcd de dos enteros:

EJERCICIO 59. Use el teorema fundamental de la aritmética para demostrar que si $a, b \in \mathbb{Z}$ se escriben como:

$$a = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \quad \text{con } r_i \geq 0,$$

$$b = p_1^{s_1} p_2^{s_2} \cdots p_m^{s_m} \quad \text{con } s_i \geq 0,$$

(donde tomamos todos los factores primos que aparecen en a y b y los ponemos en ambas factorizaciones con exponente 0 si de hecho no aparecen en uno de ellos de tal forma que $p^0 = 1$ por definición), entonces:

$$\text{mcd}(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m} \quad \text{con } \gamma_i = \text{mín}\{r_i, s_i\}.$$

El mínimo común múltiplo. Dados dos enteros a, b, distintos de cero, podemos considerar los *múltiplos comunes* de a y b (por ejemplo, el producto ab es múltiplo común de a y b). Observemos ahora que si m es múltiplo común de a y b, entonces $-m$ también es múltiplo común, por lo que existen múltiplos comunes positivos, y así, por el principio del buen orden, existe el *menor* de los múltiplos comunes positivos, al cual se llama el *mínimo común múltiplo* de a y b y lo denotaremos por $\text{mcm}[a, b]$.

LEMA III.22. *Si $a, b \in \mathbb{Z} - \{0\}$ y m es cualquier múltiplo común de a y b, entonces* $\text{mcm}[a, b]$ *divide a* m.

Demostración. Escribamos $g = \text{mcm}[a, b]$. Como $a \neq 0$ y $b \neq 0$, entonces $g \neq 0$. Si ahora dividimos m entre g y escribimos $m = gq + r$ con $0 \leq r < g$, si sucediera que $r \neq 0$ observamos que como $a|m$ y $a|g$ entonces de $r = m - gq$ se sigue que $a|r$. Similarmente $b|r$. Se sigue que r es múltiplo común positivo de a y b, pero como $r < g$ esto contradice la minimalidad de g. Se sigue que $r = 0$ por lo que $g|m$. □

EJERCICIO 60. Demuestre que $\text{mcm}[a, b] = \text{mcm}[a, -b]$.

EJERCICIO 61. Si $t > 0$ demuestre que $\text{mcm}[ta, tb] = t \cdot \text{mcm}[a, b]$.

PROPOSICIÓN III.23. *Si $a, b \in \mathbb{Z} - \{0\}$, entonces* $\text{mcm}[a, b]\text{mcd}(a, b) = |ab|$.

Demostración. Por el ejercicio (60), $\text{mcm}[a, b] = \text{mcm}[a, -b]$ y por lo tanto es suficiente probar la proposición para enteros $a > 0$ y $b > 0$.

Consideremos primero el caso cuando $\text{mcd}(a,b) = 1$ y pongamos $g = \text{mcm}[a,b]$. Como $a|g$, entonces $g = at$ con $t \in \mathbb{Z}$ y como $b|g$ entonces $b|at$; pero como $\text{mcd}(a,b) = 1$, el primer teorema de Euclides implica que $b|t$. Se sigue que $b \leq t$ y así $ab \leq at = g$. Pero como ab es múltiplo común de a y b, entonces no puede suceder que $ab < at = g$. Se debe tener entonces que $ab = at = g$, es decir,

$$\text{mcm}[a,b] = g = ab = 1 \cdot (ab) = \text{mcd}(a,b) \cdot ab.$$

Consideremos ahora el caso general, *i.e.*, cuando $\text{mcd}(a,b) = d > 1$. Dividiendo entre d se sigue que $\text{mcd}(a/d, b/d) = 1$ y aplicando el caso anterior a los enteros a/d y b/d se obtiene que

$$\text{mcm}[a/d, b/d]\text{mcd}(a/d, b/d) = \frac{a}{d}\frac{b}{d} = \frac{ab}{d^2}$$

y multiplicando esta igualdad por d^2 queda

$$d \cdot \text{mcm}[a/d, b/d]\ d \cdot \text{mcd}(a/d, b/d) = d^2 \cdot \frac{ab}{d^2},$$

es decir,

$$\text{mcm}[a,b]\text{mcd}(a,b) = ab$$

ya que $d \cdot \text{mcm}[a/d, b/d] = \text{mcm}[da/d, db/d] = \text{mcm}[a,b]$ por el ejercicio (61) y similarmente para el mcd por el ejercicio (45). □

Ejercicio 62. Con la misma notación del ejercicio (59), demuestre que:

$$\text{mcm}[a,b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_m^{\delta_m} \quad \text{con } \delta_i = \text{máx}\{r_i, s_i\}.$$

Infinitud del conjunto de primos. Si se calcula una lista de números primos, por ejemplo usando la criba de Eratóstenes, se observa que conforme crecen los primos se van haciendo escasos, de tal forma que algunas veces aparecen lagunas de enteros compuestos y esta "evidencia" empírica parece sugerir que podría haber sólo un número finito de primos. Que esto no es así lo comprueba el siguiente elegante argumento de Euclides:[5]

Teorema III.24 (Segundo teorema de Euclides). *El conjunto de primos es infinito.*

[5]Véase la proposición 20 del libro 9 de los *Elementos* de Euclides.

Demostración. Supongamos que el conjunto de primos es finito y listemos sus elementos: $2, 3, 5, \ldots, p$. Si consideramos el entero:

$$a := 2 \cdot 3 \cdot 5 \cdots p + 1$$

observamos que a no es divisible por los primos de la lista anterior, ya que al dividirlo entre cualquiera de ellos a deja residuo 1. Ahora, por el teorema fundamental de la aritmética a tiene un factor primo que por lo que vimos antes no está en la lista anterior. Esto es una contradicción. □

Ejercicio 63. Si p es un primo impar, observe que al dividirlo entre 4 deja residuo 1 o deja residuo 3. Demuestre que hay un número infinito de primos de la forma $p = 4n + 3$.

También es cierto que hay un número infinito de primos de la forma $p = 4n + 1$; sin embargo, la demostración no es tan sencilla como la que seguramente obtuvo para el caso de primos de la forma $p = 4n + 3$. ¿Podría decir dónde falla esa demostración para el caso $p = 4n + 1$?

Ejercicio 64. Demuestre que todo primo $p > 3$ es de la forma $6n + 1$ o $6n + 5$. Demuestre que hay un número infinito de primos de la forma $p = 6n + 5$.

III.6 Ecuaciones diofantinas

Diofanto de Alejandría, alrededor del siglo III de nuestra era, hizo un estudio sistemático de las soluciones enteras (o racionales) de ecuaciones con coeficientes enteros (o racionales). Algunas de estas ecuaciones ya se conocían previamente, pero fue Diofanto quien organizó los conocimientos de sus predecesores añadiendo sus propios descubrimientos y es por esto que a las ecuaciones y problemas de este tipo las llamamos ecuaciones diofantinas o problemas diofantinos. En esta sección estudiaremos ecuaciones diofantinas sencillas de la forma

$$ax + by = c \tag{1}$$

con $a, b, c \in \mathbb{Z}$ dados; es decir, estudiaremos ecuaciones diofantinas lineales en dos variables. Resolver esta ecuación quiere decir hallar todos los valores de $x, y \in \mathbb{Z}$ que al substituirlos en la ecuación anterior la vuelven una igualdad verdadera. Por ejemplo, la ecuación $2x + 3y = 10$ tiene la solución

$x = 2$, $y = 2$; pero también tiene la solución $x = -1$, $y = 4$. Más adelante veremos que, de hecho, tiene un número infinito de soluciones. En contraste, la ecuación $2x + 4y = 5$ no tiene ninguna solución entera ya que cualesquiera que sean $x, y \in \mathbb{Z}$, $2x + 4y$ es par y así no puede ser igual a 5. Esto nos muestra que antes de comenzar a buscar soluciones de las ecuaciones $ax + by = c$ es conveniente saber si tienen o no soluciones. Para esto observemos que si $x, y \in \mathbb{Z}$ son soluciones de (1), entonces $ax + by = c$ es una combinación lineal de a y b. Ahora, si $d = \text{mcd}(a, b)$, como $d|a$ y $d|b$, entonces d divide a cualquier combinación lineal de a y b y por lo tanto divide a c. Hemos así probado que si la ecuación (1) tiene soluciones en $\mathbb{Z}$, entonces $\text{mcd}(a, b)|c$. Recíprocamente, supongamos que $d = \text{mcd}(a, b)|c$. Consideremos entonces la ecuación

$$ax + by = d \qquad \text{con } d = \text{mcd}(a, b) \tag{2}$$

y notemos que como el mcd es combinación lineal de a y b (por ejemplo, usando el algoritmo de Euclides), entonces existen x_0', y_0' tales que

$$ax_0' + by_0' = d, \tag{3}$$

es decir, x_0', y_0' es una solución de la ecuación (2); hemos así mostrado que (2) siempre tiene soluciones.

Observemos ahora que como $d|c$ por hipótesis, entonces $c = dq$ con $q \in \mathbb{Z}$ y así multiplicando (3) por q se obtiene:

$$a(x_0'q) + b(y_0'q) = dq = c,$$

es decir, $x_0 := x_0'q$ y $y_0 := y_0'q$ es una solución de la ecuación (1). Hemos así probado que si $d = \text{mcd}(a, b)|c$, entonces la ecuación $ax + by = c$ tiene soluciones. De hecho hemos dado un método para hallar una de estas soluciones: usando el algoritmo de Euclides escribimos $d = \text{mcd}(a, b)$ como combinación lineal de a y b para obtener $ax_0' + by_0' = d$ y luego escribimos $c = dq$ de tal forma que $x_0 = x_0'q$ y $y_0 = y_0'q$ es una *solución particular* de $ax + by = c$.

Resumiendo, los argumentos anteriores demuestran que: *la ecuación* $ax + by = c$ *con* $a, b, c \in \mathbb{Z}$ *tiene soluciones enteras si y sólo si* $\text{mcd}(a, b)|c$.

Supongamos ahora que ya sabemos que la ecuación $ax + by = c$ tiene soluciones; con el método esbozado arriba podemos hallar una solución particular (x_0, y_0), pero ahora queremos hallar todas las soluciones. Para esto,

observemos que si (x_0, y_0) y (x_1, y_1) son dos soluciones de $ax + by = c$, entonces:

$$ax_1 + by_1 = c = ax_0 + by_0$$

por lo que $a(x_1 - x_0) + b(y_1 - y_0) = 0$, es decir, $(x_1 - x_0, y_1 - y_0)$ es solución de la ecuación

$$ax + by = 0$$

a la que llamamos una *ecuación homogénea* porque el término independiente es 0. Observamos también que cualquier ecuación homogénea siempre tiene soluciones porque $\text{mcd}(a, b)|0$. Ahora, si $(\overline{x}, \overline{y})$ es cualquier solución de la ecuación homogénea $ax + by = 0$ y si (x_0, y_0) es una solución particular de la ecuación $ax + by = c$, entonces $(x_0 + \overline{x}, y_0 + \overline{y})$ también es solución de $ax + by = c$ ya que

$$a(x_0 + \overline{x}) + b(y_0 + \overline{y}) = (ax_0 + by_0) + (a\overline{x} + b\overline{y}) = c + 0 = c.$$

Resumiendo, hemos probado que: *todas las soluciones de la ecuación* $ax + by = c$ *son de la forma*

$$x = x_0 + \overline{x}, \quad y = y_0 + \overline{y}$$

donde (x_0, y_0) *es una solución particular de* $ax + by = c$ *y* $(\overline{x}, \overline{y})$ *es cualquier solución de la ecuación homogénea asociada* $ax + by = 0$.

Así, para hallar todas las soluciones de $ax + by = c$ sólo nos falta saber cómo hallar todas las soluciones de $ax + by = 0$. Para esto último observemos que si $d = \text{mcd}(a, b)$ y $a = da'$, $b = db'$, entonces $\text{mcd}(a', b') = 1$ y se tiene que: *toda solución de* $ax + by = 0$ *es una solución de* $a'x + b'y = 0$ *y recíprocamente.* En efecto, si $(\overline{x}, \overline{y})$ es una solución de $ax + by = 0$ entonces $a\overline{x} + b\overline{y} = 0$ y así $da'\overline{x} + db'\overline{y} = 0$, por lo que cancelando d se sigue que $a'\overline{x} + b'\overline{y} = 0$, es decir, $(\overline{x}, \overline{y})$ es solución de $a'x + b'y = 0$. Recíprocamente, si $(\overline{x}, \overline{y})$ es solución de $a'x + b'y = 0$ entonces $a'\overline{x} + b'\overline{y} = 0$ y multiplicando por d se sigue que $0 = d \cdot 0 = da'\overline{x} + db'\overline{y} = a\overline{x} + b\overline{y}$, por lo que $(\overline{x}, \overline{y})$ es solución de $ax + by = 0$.

Es suficiente entonces hallar todas las soluciones de la ecuación homogénea

$$a'x + b'y = 0 \qquad \text{con } \text{mcd}(a', b') = 1.$$

Pero esto es fácil: *todas las soluciones de la ecuación* $a'x + b'y = 0$ *con* $\text{mcd}(a', b') = 1$ *son de la forma:*

$$x = b't \quad \text{y} \quad y = -a't \quad \text{con } t \in \mathbb{Z}.$$

En efecto, los números de la forma anterior son soluciones como se muestra fácilmente al substituirlos en $a'x + b'y = 0$. Recíprocamente, si $(\overline{x}, \overline{y})$ es cualquier solución de $a'x + b'y = 0$ entonces $a'\overline{x} + b'\overline{y} = 0$ por lo que $a'\overline{x} = -b'\overline{y}$, *i.e.*, $a' | -b'\overline{y}$ y como $\mathrm{mcd}(a', b') = 1$ el primer teorema de Euclides implica que $a' | -\overline{y}$ por lo que $\overline{y} = -a't$ con $t \in \mathbb{Z}$. Se sigue que $a'\overline{x} = -b'\overline{y} = -b'(-a't) = a'b't$ de donde cancelando a' se obtiene que $\overline{x} = b't$ como se quería.

Resumiendo, hemos probado:

PROPOSICIÓN III.25. *Si $a, b \in \mathbb{Z} - \{0\}$, la ecuación diofantina $ax + by = c$ tiene soluciones enteras si y sólo si $\mathrm{mcd}(a, b) | c$. Más aún, todas las soluciones son de la forma:*

$$\begin{aligned} x &= x_0 + b't \qquad \text{con} \qquad b = b'd, \ \ d = \mathrm{mcd}(a, b) \\ y &= y_0 - a't \qquad \text{con} \qquad a = a'd, \ \ d = \mathrm{mcd}(a, b) \end{aligned}$$

con $t \in \mathbb{Z}$ arbitrario y con (x_0, y_0) una solución particular de $ax + by = c$ que se puede hallar con el algoritmo de Euclides. □

Ejemplo 6. Hallar todas las soluciones de la ecuación diofantina $4x + 6y = 8$. En este ejemplo $\mathrm{mcd}(4, 6) = 2$ y $2|8$ por lo que sí existen soluciones. Para hallar una solución particular escribimos al máximo común divisor 2 como combinación lineal: $2 = 4(-1) + 6(1)$; ahora, como $8 = 2(4)$, multiplicamos por 4 para obtener la solución particular $x_0 = 4(-1) = -4$, $y_0 = 4(1) = 4$ de $4x + 6y = 8$. Dividiendo los coeficientes de la ecuación por el $\mathrm{mcd}(4, 6) = 2$, se obtiene la ecuación homogénea $2x + 3y = 0$ cuyas soluciones son $x = 3t$, $y = -2t$ con $t \in \mathbb{Z}$. Así, las soluciones de la ecuación dada $4x + 6y = 8$ son

$$x = -4 + 3t, \quad y = 4 - 2t \quad \text{con } t \in \mathbb{Z}.$$

EJERCICIO 65. Encuentre todas las soluciones de las ecuaciones diofantinas siguientes:

(I) $243x + 198y = 9$.

(II) $43x + 64y = 1$.

(III) $6x + 10y = 1$.

(IV) $35x + 17y = 14$.

(v) $15x + 21y = 10$.

(vi) $71x - 50y = 1$.

(vii) $93x + 81y = 3$.

III.7 Congruencias y aritmética modular

Dado un entero $m \geq 1$ fijo, usando la divisibilidad en $\mathbb{Z}$, definimos la relación siguiente en $\mathbb{Z}$: dados dos enteros $a, b \in \mathbb{Z}$, diremos que a *es congruente con* b *según el módulo* m, si $m|a - b$. Usaremos la notación $a \equiv b$ mód m para indicar que $m|a - b$. Nótese que así decir que $a \equiv 0$ mód m es lo mismo que decir que $m|a$.

Lema III.26. *Fijo un entero* $m \geq 1$, *la relación de congruencia módulo* m *es una relación de equivalencia en* $\mathbb{Z}$.

Demostración. Es reflexiva ya que si $a \in \mathbb{Z}$ entonces $m|a - a = 0$ por lo que $a \equiv a$ mód m.

Es simétrica ya que si $a \equiv b$ mód m, entonces $m|a - b$, *i.e.*, $a - b = mq$ por lo que $b - a = m(-q)$ y así $m|b - a$, *i.e.*, $b \equiv a$ mód m.

Es transitiva ya que si $a \equiv b$ mód m y $b \equiv c$ mód m, entonces $m|a - b$ y $m|b - c$ por lo que $m|(a - b) + (b - c) = a - c$, *i.e.*, $a \equiv c$ mód m. □

Ejemplo 7. Si $m = 2$ y $a, b \in \mathbb{Z}$, la relación $a \equiv b$ mód m quiere decir que a y b tienen la misma *paridad*, es decir, ambos son pares o ambos son impares.

Las propiedades siguientes se verifican fácilmente:

Proposición III.27. *Sea* $m \geq 1$ *un entero fijo. Entonces:*

(1) *Si* $a \equiv b$ mód m *y* $c \in \mathbb{Z}$, *entonces* $a + c \equiv b + c$ mód m.

(2) *Si* $a \equiv b$ mód m *y* $c \in \mathbb{Z}$, *entonces* $ac \equiv bc$ mód m.

(3) *Si* $a \equiv b$ mód m *y* $a' \equiv b'$ mód m, *entonces* $a + a' \equiv b + b'$ mód m.

(4) *Si* $a \equiv b$ mód m *y* $a' \equiv b'$ mód m, *entonces* $aa' \equiv bb'$ mód m.

Demostración. (1) Como $m|a-b$ entonces $m|(a-b) = (a+c)-(b+c)$.

(2) Como $m|a-b$ entonces $m|c(a-b) = ac-bc$.

(3) Aplicando (1) con $c = a'$ y $a \equiv b$ mód m se sigue que

$$a + a' \equiv a' + b \text{ mód } m \tag{I}$$

y aplicando (1) con $c = b$ y $a' \equiv b'$ mód m se sigue que

$$a' + b \equiv b + b' \text{ mód } m \tag{II}$$

y usando las congruencias (I) y (II) y la transitividad de la relación de congruencia, se sigue que $a + a' \equiv b + b'$ mód m.

(4) Se demuestra como la parte (3) aplicando ahora la parte (2). □

EJERCICIO 66. Si $a \equiv b$ mód m y $d|m$. $d > 0$, demuestre que $a \equiv b$ mód d.

EJERCICIO 67. Demuestre que si $ax \equiv ay$ mód m y $\text{mcd}(a, m) = 1$, entonces $x \equiv y$ mód m.

EJERCICIO 68. Demuestre que si $x \quad y$ mód m, entonces $\text{mcd}(x, m) = \text{mcd}(y, m)$.

Consideremos ahora el conjunto cociente de la relación de congruencia mód m; denotaremos a este conjunto cociente mediante $\mathbb{Z}/m\mathbb{Z}$ y para describir a este conjunto describiremos a sus clases de equivalencia. Sea $a \in \mathbb{Z}$; su clase de equivalencia mód m es el conjunto:

$$[a] := \{x \in \mathbb{Z} \ : \ x \equiv a \text{ mód } m\}.$$

Así, si $x \in [a]$ entonces $a \equiv x$ mód m por lo que $m|a-x$, es decir, $a-x = mq$ para algún $q \in \mathbb{Z}$. Se sigue que $a = mq + x$. Esta igualdad nos recuerda al algoritmo de la división cuando dividimos a entre m. Sin embargo, en general, no sabemos que x sea el residuo de esta división. Si ahora hacemos la división de a entre m y obtenemos

$$a = mq + r \quad \text{con } 0 \leq r < m$$

observamos que $a - r = mq$ por lo que $a \equiv r \pmod{m}$. Entonces, para cualquier $x \in [a]$ se tiene que $x \equiv a \pmod{m}$ y como $a \equiv r \pmod{m}$, por transitividad se sigue que $x \equiv r \pmod{m}$, *i.e.*, $x - r = mt$ por lo que $x = mt + r$ con $0 \leq r < m$; es decir, el residuo de dividir cualquier $x \in [a]$ por m es el mismo residuo r que resulta al dividir a entre m. Ahora, como m está fijo, entonces sólo hay un número finito de posibilidades para el residuo r que queda al dividir cualquier entero a entre m, a saber:

$$r = 0, 1, 2, \ldots, (m-1).$$

Por lo tanto a lo más sólo hay m clases de equivalencia en $\mathbb{Z}/m\mathbb{Z}$:

$$[0], [1], [2], \ldots, [m-1]$$

y es claro que estas clases son distintas ya que un entero a no puede dejar residuos distintos al dividirlo entre m. Se sigue que

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \ldots, [m-1]\}.$$

Nuestro objetivo ahora es introducir una estructura de anillo (conmutativo con uno) en $\mathbb{Z}/m\mathbb{Z}$ al que llamaremos el *anillo de enteros módulo* m. Las operaciones que necesitamos se definen como sigue: dadas dos clases de equivalencia $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$ (a las que llamaremos *clases residuales módulo* m), escojamos elementos $a \in [a]$ y $b \in [b]$ a los que llamaremos *representantes* de las clases respectivas. Se define entonces:

SUMA. Los representantes elegidos se suman en $\mathbb{Z}$ para obtener $a + b \in \mathbb{Z}$ y luego se toma la clase de equivalencia correspondiente $[a + b]$ y se define:

$$[a] + [b] := [a + b].$$

Que esta definición no depende de los representantes elegidos es el contenido de la parte (1) del lema siguiente.

PRODUCTO. Los representantes elegidos se multiplican en $\mathbb{Z}$ para obtener $ab \in \mathbb{Z}$ y luego se toma la clase de equivalencia correspondiente $[ab]$ y se define:

$$[a] \cdot [b] := [ab].$$

Que esta definición no depende de los representantes elegidos es el contenido de la parte (2) del lema siguiente.

LEMA III.28. *Sea $m \geq 1$ un entero fijo. Si $a, a' \in [a]$ y $b, b' \in [b]$, entonces:*

(1) $[a + b] = [a' + b']$.

(2) $[ab] = [a'b']$.

Demostración. Se sigue directo de las partes (3) y (4) de la proposición (III.27). □

TEOREMA III.29. *Sea $m \geq 1$ un entero fijo. Con las operaciones definidas arriba $\mathbb{Z}/m\mathbb{Z}$ es un anillo conmutativo con uno.*

Demostración. Que la suma es asociativa y conmutativa lo dejamos como un ejercicio. El neutro aditivo de $\mathbb{Z}/m\mathbb{Z}$ es la clase residual $[0]$ ya que $[a]+[0] = [a + 0] = [a]$ para todo $[a]$. El inverso aditivo de $[a] \in \mathbb{Z}/m\mathbb{Z}$ es la clase residual $[-a]$ ya que $[a] + [-a] = [a - a] = [0]$. Nótese que $[-a] = [m - a]$.

Que el producto es asociativo, conmutativo y distribuye a la suma lo dejamos como un ejercicio. El neutro multiplicativo de $\mathbb{Z}/m\mathbb{Z}$ es la clase $[1]$. □

EJERCICIO 69. Demuestre la asociatividad y conmutatividad de la suma en $\mathbb{Z}/m\mathbb{Z}$. Demuestre la asociatividad y conmutatividad del producto en $\mathbb{Z}/m\mathbb{Z}$. Demuestre la distributividad en $\mathbb{Z}/m\mathbb{Z}$.

Veamos algunos ejemplos, para acostumbrarnos a la aritmética de $\mathbb{Z}/m\mathbb{Z}$, a la que algunas veces se le conoce como *aritmética modular*:

Ejemplo 8. En $\mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$ se tiene que $[4] + [5] = [3]$ ya que $4 + 5 = 9 = (6)(1) + 3$. Otro ejemplo es $[3][4] = [0]$ ya que el residuo de dividir $(3)(4) = 12$ entre 6 es 0.

Ejemplo 9. La aritmética de $\mathbb{Z}/12\mathbb{Z}$ es la aritmética del reloj de manecillas de 12 horas; por ejemplo, si sumamos 5 horas a las 11 de la mañana, el resultado es las 4 de la tarde. Esto es así porque, en $\mathbb{Z}/12\mathbb{Z}$, se tiene que $[5] + [11] = [4]$ ya que $5 + 11 = 16$ que al dividirlo entre 12 deja residuo 4.

Ejemplo 10. En las computadoras de no hace mucho tiempo, los registros de memoria eran de 8 bits, es decir, los registros de memoria de la computadora estaban compuestos por 8 casillas donde la computadora almacenaba ceros o unos:

La computadora es binaria, por lo que los números los maneja en base 2; si no recuerda cómo expresar un número en base 2, véase en la sección sobre criptografía (III.9, pp. 174 y ss.) cómo es la expansión en base 2 de cualquier entero. Por ejemplo, en base 2, el símbolo 1100 representa al número doce; así, al sumar uno al doce obtenemos $1100 + 1 = 1101$ que es el número 13. Por otro lado, si sumamos $1101 + 1 = 1110$, o lo que es lo mismo $13 + 1 = 14$. Similarmente, $1110 + 1 = 1111$, *i.e.*, $14 + 1 = 15$. Ahora, $1111 + 1 = 10000$, es decir, $15 + 1 = 16$. Estos ejemplos nos muestran que, dado un número de cuatro dígitos binarios, al irle sumando 1 seguimos obteniendo un número de cuatro dígitos mientras haya ceros en el número al que le sumamos el 1; sin embargo, cuando el número de cuatro dígitos tiene sólo unos, *i.e.*, es 1111, al sumarle 1 convierte estos cuatro dígitos en ceros y pone un 1 a la izquierda.

Ahora, para el caso de la máquina con registros de 8 bits, éstos pueden almacenar números binarios con ocho dígitos y así no tienen problemas para sumar 1 mientras haya ceros; sin embargo, cuando las ocho casillas de estos registros están ocupadas por unos y se tiene un 1 extra para almacenar en memoria, al sumar este 1 al número formado por los ocho unos 11111111 (en base 2 este número es 255) todas las casillas se convierten en ceros, porque no hay lugar para almacenar el 1 de la izquierda. Dicho en otras palabras, para la máquina $11111111 + 1 = 0$, *i.e.*, $255 + 1 = 0$, es decir, para la máquina $256 = 0$ y esto sucede porque la computadora de ocho bits está trabajando con aritmética modular en $\mathbb{Z}/256\mathbb{Z}$.

Observación. En general $\mathbb{Z}/m\mathbb{Z}$ no es un dominio entero. Por ejemplo, en $\mathbb{Z}/6\mathbb{Z}$ se tiene que $[2] \neq [0]$ y $[3] \neq [0]$ pero $[2][3] = [6] = [0]$.

TEOREMA III.30. *$\mathbb{Z}/p\mathbb{Z}$ es un dominio entero si y sólo si p es primo.*

Demostración. ($\Leftarrow$): Si p es primo, sean $[a], [b] \in \mathbb{Z}/p\mathbb{Z}$ tales que $[a][b] = [0]$. Entonces, $ab \equiv 0$ mód p por lo que $p|ab$. Pero como p es primo esto implica que $p|a$ o $p|b$, es decir, $a \equiv 0$ mód p o $b \equiv$ mód p, *i.e.*, $[a] = [0]$ o $[b] = [0]$.

($\Rightarrow$): Si p no fuera primo entonces existirían enteros a, b tales que $1 < a < p$ y $1 < b < p$ y $p = ab$. Se tendría entonces que $[a][b] = [p] = [0]$ con $[a] \neq [0]$ y $[b] \neq [0]$, en contradicción con la hipótesis de que $\mathbb{Z}/p\mathbb{Z}$ es dominio entero. □

En el ejercicio 23 mostramos que los únicos elementos del anillo $\mathbb{Z}$ que tienen inverso multiplicativo son 1 y -1. Para los anillos $\mathbb{Z}/m\mathbb{Z}$, ¿cuáles

elementos tienen inverso multiplicativo? Para responder a esta pregunta supongamos que el elemento $[u] \in \mathbb{Z}/m\mathbb{Z}$ tiene inverso multiplicativo. Este inverso multiplicativo es un elemento $[v] \in \mathbb{Z}/m\mathbb{Z}$ tal que $[u][v] = [1]$, es decir, $uv \equiv 1$ mód m y así $uv - 1 = mt$ para algún $t \in \mathbb{Z}$. Se sigue que $uv - mt = 1$, en particular 1 es combinación lineal de m y u por lo que $\text{mcd}(u, m) = 1$. Recíprocamente, si $\text{mcd}(u, m) = 1$ entonces $1 = us + mt$ por lo que $[1] = [us + mt] = [u][s] + [m][t] = [u][s]$ ya que $[m] = [0]$. Se sigue que $[u]$ tiene inverso multiplicativo $[s]$. Hemos así probado:

PROPOSICIÓN III.31. *Si $m \geq 1$, entonces $[u] \in \mathbb{Z}/m\mathbb{Z}$ tiene inverso multiplicativo si y sólo si* $\text{mcd}(u, m) = 1$. □

Ejemplo 11. Si $m = p$ es primo, ¿cuáles elementos de $\mathbb{Z}/p\mathbb{Z}$ tienen inverso multiplicativo? Sabemos que $[u] \in \mathbb{Z}/p\mathbb{Z}$ tiene inverso multiplicativo si y sólo si $\text{mcd}(u, p) = 1$, pero como p es primo, esto sucede si y sólo si $p \nmid u$. Entonces, los elementos de $\mathbb{Z}/p\mathbb{Z}$ que tienen inverso multiplicativo son todos excepto el $[0]$. Por otra parte es claro que el cero de un anillo (no trivial) nunca puede tener inverso multiplicativo. ¿Por qué?

Dado A un anillo conmutativo con 1, denotamos al conjunto de elementos con inverso multiplicativo mediante A^*. Así, en el ejemplo anterior se tiene que

$$(\mathbb{Z}/p\mathbb{Z})^* = \{[1], [2], [3], \ldots, [p-1]\}.$$

Ejemplo 12. Si $m = 4$, ¿cuáles elementos de $\mathbb{Z}/4\mathbb{Z}$ tienen inverso multiplicativo? Para comenzar, el uno de cualquier anillo conmutativo siempre tiene inverso multiplicativo, a saber, él mismo. Así $[1]$ tiene inverso multiplicativo. El $[2]$ no tiene inverso multiplicativo porque no es coprimo con 4 y el $[3]$ sí tiene inverso multiplicativo porque 3 es coprimo con 4. Se tiene entonces que $(\mathbb{Z}/4\mathbb{Z})^* = \{[1], [3]\}$.

EJERCICIO 70. Calcule $(\mathbb{Z}/6\mathbb{Z})^*$ y $(\mathbb{Z}/8\mathbb{Z})^*$.

Un anillo conmutativo con uno K, en el cual $1 \neq 0$, tal que todos los elementos de K excepto el 0 tienen inverso multiplicativo (*i.e.*, $K^* = K - \{0\}$) se llama un *campo*. Así, arriba mostramos que si p es primo entonces $\mathbb{Z}/p\mathbb{Z}$ es un campo. Más adelante encontraremos otros ejemplos de campos.

Como en general $\mathbb{Z}/m\mathbb{Z}$ no es un dominio entero, la ley de cancelación para el producto no es válida en general en $\mathbb{Z}/m\mathbb{Z}$. Por ejemplo, en $\mathbb{Z}/6\mathbb{Z}$ se tiene que

$$[2][3] = [0] = [2][0]$$

y sin embargo $[3] \neq [0]$, es decir no podemos cancelar el factor $[2]$ en la igualdad de arriba. Podríamos entonces preguntarnos por cuáles factores de $\mathbb{Z}/m\mathbb{Z}$ se pueden cancelar:

EJERCICIO 71. Si $m \geq 1$ es fijo y $[a], [b], [c] \in \mathbb{Z}/m\mathbb{Z}$ son tales que $[a][c] = [b][c]$ y además $\text{mcd}(c, m) = 1$ (*i.e.*, $[c] \in (\mathbb{Z}/m\mathbb{Z})^*$), demuestre que $[a] = [b]$.

III.8 CONGRUENCIAS LINEALES

Si $m \geq 1$ es un entero fijo, una congruencia lineal es una congruencia de la forma

$$(*) \qquad ax \equiv b \text{ mód } m$$

con $a, b \in \mathbb{Z}$ dados y $[a] \neq [0]$, *i.e.*, $a \not\equiv 0$ mód m; la letra x denota un entero por determinar y decimos que es una incógnita. Resolver la congruencia $(*)$ quiere decir hallar los valores de x que al substituirlos en $(*)$ la vuelven verdadera.

Notemos que $ax \equiv b$ mód m quiere decir que $ax - b = my$, para algún $y \in \mathbb{Z}$. Se tiene así la ecuación diofantina

$$(\dagger) \qquad ax - my = b$$

con $a, m, b \in \mathbb{Z}$ dados. Observamos ahora que para cada solución x de $(*)$ se tiene que $ax - b = my$ con $y \in \mathbb{Z}$ y así se tiene la solución (x, y) de $(\dagger)$. Recíprocamente, para toda solución (x, y) de $(\dagger)$ desechando la y se tiene la solución x de $(*)$. Entonces, para hallar las soluciones de la congruencia $(*)$ resolvemos la ecuación diofantina $(\dagger)$ y de estas soluciones (x, y) desechamos las y. Ahora como ya sabemos que la ecuación diofantina $(\dagger)$ tiene soluciones si y sólo si $\text{mcd}(a, m) | b$ y cuando esto sucede la coordenada x de las soluciones (x, y) es de la forma

$$x = x_0 + m't \qquad \text{con } m = m'd, \ \ d = \text{mcd}(a, m),$$

entonces:

TEOREMA III.32. *La congruencia lineal* $ax \equiv b$ mód m *tiene soluciones en* $\mathbb{Z}$ *si y sólo si* $\mathrm{mcd}(a,m)|b$. *Cuando hay soluciones estas tienen la forma siguiente:*

$$x = x_0 + m't \quad \text{con } m = m'd,\ d = \mathrm{mcd}(a,m),$$

donde x_0 *es cualquier solución particular de la congruencia. Podemos escribir estas soluciones como:*

$$x \equiv x_0 + m't \ (\text{mód } m) \qquad \text{con } m' = m/d,\ \ d = \mathrm{mcd}(a,m) \text{ y } t \in \mathbb{Z}. \qquad \square$$

Si lo que queremos son todas las *soluciones distintas* módulo m de la congruencia $ax \equiv b$ mód m, necesitaremos la generalización siguiente del ejercicio (67):

LEMA III.33. *Sea* $g = \mathrm{mcd}(a,m)$. *Entonces,* $ax \equiv ay$ (mód m) *si y sólo si* $x \equiv y$ (mód (m/g)).

Demostración. ($\Rightarrow$): Si $ax \equiv ay$ (mód m), entonces $a(x-y) = mz$ para algún $z \in \mathbb{Z}$ y como $g|m$ y $g|a$ entonces $(a/g)(x-y) = (m/g)z$ por lo que $(m/g)|(a/g)(x-y)$. Pero como a/g y m/g son coprimos, de la última divisibilidad se sigue que $(m/g)|(x-y$, *i.e.,* $x \equiv y$ (mód (m/g)).

($\Leftarrow$): Si $x \equiv y$ (mód (m/g)), entonces $(m/g)|(x-y)$, *i.e.,* $x - y = (m/g)q$ y así $g(x-y) = mq$ por lo que $m|g(x-y)$. Pero como $g|a$, entonces $g(x-y)|a(x-y)$ y así, por transitividad $m|a(x-y)$, *i.e.,* $ax \equiv ay$ (mód m). $\square$

Nótese que el ejercicio (67) se sigue de este lema poniendo $g = 1$. De esta observación obtendremos el número de soluciones distintas módulo m de una congruencia lineal en el caso en que el coeficiente a y el módulo m son coprimos:

COROLARIO III.34. *Si* $\mathrm{mcd}(a,m) = 1$, *entonces la congruencia* $ax \equiv b$ mód m *tiene una única solución* x_0 *módulo* m, *es decir, todas sus soluciones son de la forma* $x = x_0 + tm$ *con* $t \in \mathbb{Z}$.

Demostración. Como $\mathrm{mcd}(a,m) = 1|b$, entonces por el teorema anterior la congruencia tiene soluciones. Ahora, si x_0 y x_1 son dos soluciones cualesquiera, entonces $ax_0 \equiv ax_1$ mód m, y así, por el lema anterior $x_0 \equiv x_1$ mód m. $\square$

En el caso general, cuando $g = \text{mcd}(a, m)|b$, observemos que $u \in \mathbb{Z}$ es solución de la congruencia $ax \equiv b$ mód m si y sólo si $au \equiv b$ mód m, pero esto último sucede si y sólo si $(a/g)u \equiv (b/g)$ mód (m/g). Ahora, como $\text{mcd}(a/g, m/g) = 1$, por el corolario anterior la congruencia $(a/g)u \equiv (b/g)$ mód (m/g) tiene una única solución, digamos x_0, módulo m/g, *i.e.*, $x = x_0 + t(m/g)$ son todas sus soluciones con x_0 una solución particular de $(a/g)u \equiv (b/g)$ mód (m/g). Así, todas las soluciones de $ax \equiv b$ mód m son de la forma $u = x_0 + t(m/g)$ con $t \in \mathbb{Z}$. Por otra parte observamos que si $0 \leq t \leq g - 1$, de las soluciones correspondientes $u = x_0 + t(m/g)$ ningún par de ellas son congruentes módulo m y si t toma otro valor distinto de los anteriores, dividiéndolo entre g se sigue que la solución correspondiente será congruente a alguna de las anteriores. Hemos así probado que todas las soluciones distintas módulo m de $ax \equiv b$ mód m son de la forma

$$x = x_0 + t(m/g) \qquad \text{con } 0 \leq t \leq g - 1,\ g = \text{mcd}(a, m),$$

donde x_0 es la única solución de la congruencia $(a/g)x \equiv (b/g)$ mód (m/g).

Ejemplo 13. Para hallar todas las soluciones de la congruencia $2x \equiv 3$ mód 5, comenzamos observando que $\text{mcd}(2, 5) = 1|3$ por lo que sí hay soluciones. Para hallar estas soluciones consideramos la ecuación diofantina $2x - 5y = 3$ y como $1 = \text{mcd}(2, -5)$ escribimos al 1 como combinación lineal de 2 y -5, digamos $1 = 2(-2) - 5(-1)$ y luego como el término independiente de la ecuación diofantina es $3 = 1(3)$ donde $1 = \text{mcd}(2, -5)$, multiplicamos por 3 para obtener $3 = 3(1) = 3(2(-2) - 5(-1) = 2(-6) - 5(-3)$ por lo que $x_0 = -6$ y $y_0 = -3$ es una solución particular de $2x - 5y = 3$. Desechando la y, se sigue que la solución general de la congruencia $2x \equiv 3$ mód 5 es:

$$x = -6 + 5t \quad \text{con } t \in \mathbb{Z}.$$

En algunas ocasiones nos pueden pedir que escojamos una solución particular x_0 positiva. En este ejemplo poniendo $t = 2$ se obtiene $x_0 = -6 + 5(2) = 4$.

Ejercicio 72. Encuentre todas las soluciones de las congruencias lineales siguientes:

(i) $16x \equiv 9$ mód 35.

(ii) $200x + 135 \equiv 0$ mód 441.

(III) $20x \equiv 4$ mód 30.

(IV) $20x \equiv 30$ mód 4.

Para su uso en el tema siguiente necesitaremos:

LEMA III.35. *Si* $m_i \geq 1$, *para* $1 \leq i \leq k$, *entonces:*

$$x \equiv y \text{ mód } m_i \quad \text{para } 1 \leq i \leq k \Leftrightarrow x \equiv y \text{ mód } (\text{mcm}[m_1, \ldots, m_k]).$$

Demostración. ($\Rightarrow$): Como $m_i | x - y$ para todo $i = 1, \ldots, k$, entonces $x - y$ es múltiplo común de todos los m_i y por lo tanto $\text{mcm}[m_1, \ldots, m_k]$ divide a $x - y$, *i.e.*, $x \equiv y$ mód $(\text{mcm}[m_1, \ldots, m_k])$.

($\Leftarrow$): Como $\text{mcm}[m_1, \ldots, m_k]$ divide a $x-y$, y m_i divide a $\text{mcm}[m_1, \ldots, m_k]$, entonces por transitividad $m_i | x - y$ para toda i, es decir, $x \equiv y$ mód m_i para toda i. □

Hemos visto hasta ahora que para resolver una congruencia lineal $ax \equiv b$ mód m el método es escribir a $d = \text{mcd}(a, m)$ como combinación lineal de a y b, digamos $d = as - mr$, y luego escribir $b = dq$ para hallar $x_0 = sq$ como solución particular de la congruencia. Después se escribe $m = m'd$ para que al final se tengan todas las soluciones de la forma $x = x_0 + m't$. Cuando a y m son pequeños el método anterior es práctico, como vimos en el ejemplo 13 arriba. Sin embargo, cuando estos números son grandes el algoritmo de Euclides puede ser muy largo. Una forma de facilitar lo anterior es factorizar el módulo m en producto de primos $m = \prod_{i=1}^{k} p_i^{e_i}$ y observar que los factores $m_i = p_i^{e_i}$ son coprimos por pares y así, por el lema (III.35) se sigue que el problema de resolver la congruencia $ax \equiv b$ mód m es equivalente a resolver el conjunto de congruencias $ax \equiv b$ mód m_i para $1 \leq i \leq k$ ya que $m = \text{mcm}[m_1, \ldots, m_k]$ porque $\text{mcd}(m_i, m_j) = 1$ si $i \neq j$. Ahora, las congruencias $ax \equiv b$ mód m_i en principio son más sencillas que la congruencia original $ax \equiv b$ mód m ya que m_i es menor que m. Supongamos que resolvimos todas las congruencias $ax \equiv b$ mód m_i, *i.e.*, que éstas tienen como soluciones a $x \equiv u_i$ mód m_i. El problema ahora es hallar una u que sea solución simultánea de todas las congruencias $x \equiv u_i$ mód m_i, de tal forma que esta u será la solución buscada de $ax \equiv b$ mód m. Hemos reducido así el problema a resolver un sistema de congruencias de la forma

$$x \equiv u_i \text{ mód } m_i, \quad 1 \leq i \leq k.$$

Estos sistemas de congruencias fueron estudiados en el siglo I de nuestra era por el matemático chino Sun-Tsu, en la forma, por ejemplo, de encontrar un número x que al dividirlo entre 3, 5 y 7 deje residuos 2, 3 y 2, respectivamente, con la única condición de que los números entre los que se divida, los módulos, sean coprimos por parejas:

TEOREMA III.36 (Teorema chino del residuo). *Supongamos que $m_1, \ldots, m_k$ son enteros positivos coprimos por parejas y sean $a_1, \ldots, a_k$ enteros arbitrarios. Entonces, el sistema de congruencias*

$$x \equiv a_i \text{ mód } m_i, \quad 1 \leq i \leq k$$

tiene una solución común u. Más aún, cualesquiera dos soluciones u, v del sistema de congruencias anterior satisfacen que

$$u \equiv v \text{ mód } (m_1 \cdots m_k).$$

Demostración. Pongamos $m = m_1 \cdots m_k$. Entonces, cada m/m_j es un entero y además $\text{mcd}(m/m_j, m_j) = 1$ ya que $\text{mcd}(m_i, m_j) = 1$ si $i \neq j$. Entonces, las congruencias

$$(m/m_j)x \equiv 1 \text{ mód } m_j$$

tienen solución, digamos b_j. Es claro también que $(m/m_j)b_j \equiv 0$ mód m_i si $i \neq j$ ya que $m_i|(m/m_j)$ en este caso. Pongamos ahora

$$x_0 := \sum_{j=1}^{k} (m/m_j)b_j a_j$$

y observemos que

$$\begin{aligned} x_0 = \sum_{j=1}^{k} (m/m_j)b_j a_j &\equiv (m/m_i)b_i a_i \text{ mód } m_i \\ &\equiv a_i \text{ mód } m_i \end{aligned}$$

ya que $(m/m_i)b_i \equiv 1$ mód m_i. Por lo tanto x_0 es solución de las congruencias $x \equiv a_i$ mód m_i.

Supongamos ahora que x_0 y x_1 son soluciones del sistema de congruencias $x \equiv a_i$ mód m_i. Entonces $x_0 \equiv x_1$ mód m_i para $1 \leq i \leq k$, por lo que $x_0 \equiv x_1$ mód $(\text{mcm}[m_1, \ldots, m_k])$ por el lema (III.35). Se sigue que $x_0 \equiv x_1$ mód m ya que $m = m_1 \cdots m_k = \text{mcm}[m_1, \ldots, m_k]$. □

Ejemplo 14. Resuelva el sistema de congruencias

$$x \equiv 8 \text{ mód } 11$$
$$x \equiv 3 \text{ mód } 19.$$

Las soluciones de la primera congruencia son de la forma $x = 8 + 11u$. Substituyendo estas soluciones en la segunda congruencia obtenemos $8 + 11u \equiv 3$ mód 19 que al simplificar queda $11u \equiv -5$ mód 19 y esta congruencia la sabemos resolver. Sus soluciones son de la forma $u = 3 + 19t$. Se sigue que las soluciones del sistema de congruencias son

$$x = 8 + 11u = 8 + 11(3 + 19t) = 8 + 33 + 11(19)t = 41 + (11)(19)t$$

con $t \in \mathbb{Z}$.

EJERCICIO 73. Resuelva los sistemas de congruencias:

(1) $x \equiv 3$ mód 7 y $x \equiv 5$ mód 9.
(2) $x \equiv 5$ mód 7 y $x \equiv 2$ mód 12 y $x \equiv 8$ mód 13.
(3) $x \equiv 3$ mód 37 y $x \equiv 1$ mód 87.

Use congruencias para resolver los ejercicios siguientes, que son resultados que usamos desde la escuela elemental:

EJERCICIO 74. Sea $x \in \mathbb{Z}$. Demuestre que $3|x$ si y sólo si la suma de los dígitos de x es divisible entre 3.

EJERCICIO 75. Sea $x \in \mathbb{Z}$. Demuestre que $9|x$ si y sólo si la suma de los dígitos de x es divisible entre 9.

EJERCICIO 76. Sea $x \in \mathbb{Z}$. Demuestre que x es par si y sólo si el dígito de unidades (último dígito) de x es par.

EJERCICIO 77. Sea $x \in \mathbb{Z}$. Demuestre que $4|x$ si y sólo si el entero formado por sus dígitos de decenas y unidades es divisible entre 4.

EJERCICIO 78 (Dígitos de verificación). A todos los libros que se publican, se les asigna un número de 9 dígitos que los clasifica en forma única. En este número, llamado el ISBN, los primeros dígitos identifican el país y la

editorial que publica el libro. Si la lectora o lector se fija en la página legal de cualquier libro (usualmente, la página 6) o en la cubierta posterior, podrá ver el ISBN que identifica el libro; observe también que el ISBN tiene la forma

968-16-7826-5

es decir, se ha añadido un décimo dígito, usualmente después de un *guión* (en el ejemplo anterior es el número 5). Este décimo dígito es el *dígito de verificación* que, como su nombre lo indica, verifica que el ISBN se generó e imprimió correctamente, y se obtiene como sigue: si

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9\text{-}v$$

es cualquier ISBN con dígito de verificación v, entonces

$$1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 \equiv v \text{ (mód 11)}.$$

Note que como los residuos módulo 11 pueden ser del 0 al 10, estos diez dígitos se denotan : 0, 1, 2, 3, ..., 8, 9, X, donde X denota al dígito 10. Busque entre sus libros alguno que tenga el dígito de verificación X y compruebe que el ISBN se obtuvo correctamente.[6]

Se invita al lector o lectora interesados a investigar otras instancias donde se usen dígitos de verificación.

III.9 Proyecto 2: Criptografía de clave pública

En este proyecto se esbozan algunas ideas que desarrollan temas similares a los estudiados en este capítulo y al final se aplican al desarrollo de un criptosistema que se usa para la protección de información. La base de este criptosistema es un resultado aritmético descubierto por el matemático francés Pierre de Fermat alrededor del año 1640, y es relativamente fácil de re-descubrir: dado cualquier entero a y un natural $m \geq 2$, podemos considerar las potencias a, a^2, a^3, ..., módulo el entero m y buscar un patrón en estas potencias (por supuesto que sólo interesan los enteros $a \neq 0$). En el caso cuando $m = p$ es un primo, este patrón es fácil de visualizar, por ejemplo, para $p = 5$ y $p = 7$ las tablas siguientes listan unas potencias a^k (mód p) para algunos enteros $a = 1, 2, 3, \ldots$:

[6] A partir de enero de 2007 constarán de 13 dígitos (incluyendo el verificador). A los ISBN actuales se les añadirá el número 978. Obviamente, el dígito verificador cambiará.

a	a^2	a^3	a^4	a^5
1	1	1	1	1
2	4	3	1	2
3	4	2	1	3
4	1	4	1	4

a^k módulo 5

a	a^2	a^3	a^4	a^5	a^6	a^7
1	1	1	1	1	1	1
2	4	1	2	4	1	2
3	2	6	4	5	1	3
4	2	1	4	2	1	4
5	4	6	2	3	1	5
6	1	6	1	6	1	6

a^k módulo 7

Mirando estas tablas notamos de inmediato las columnas que consisten en unos, a saber, las columnas a^4 (mód 5) y a^6 (mód 7). Unos cuantos ejemplos más nos convencerían de que, en general, $a^{p-1} \equiv 1$ (mód p) para todo entero a tal que $1 \leq a < p$. Este es el *pequeño* teorema que Fermat comunicó a Frénicle de Bessy en una carta del 18 de octubre de 1640. Por supuesto que no es necesario restringirse a enteros a entre 1 y $p-1$, ya que si a_1 y a_2 difieren por un múltiplo de p, digamos $a_1 = a_2 + pt$, entonces las potencias a_1^k y a_2^k son iguales mód p, como Fermat mismo podría haber demostrado, por ejemplo usando el teorema del binomio, algo que Fermat ya había estudiado desde 1636, posiblemente siguiendo a Viète. Así, la condición importante sobre el entero a es que no sea congruente con 0 módulo p, *i.e.,* que no sea un múltiplo de p. Usando la notación de congruencias, debida a Gauss, el (pequeño)[7] teorema de Fermat se formula como sigue:

[7]Se suele llamar *pequeño* a este teorema para distinguirlo del *gran* teorema de Fermat, que en realidad es la famosa *conjetura de Fermat*: para $n \geq 3$, la ecuación $x^n + y^n = z^n$ sólo tiene las soluciones enteras triviales, *i.e.,* con $xyz = 0$. Esta conjetura fue demostrada en 1994, ¡más de 350 años después de haber sido soñada por Fermat!

TEOREMA III.37 (Fermat). *Sea p un primo. Entonces, para cualquier entero a no divisible por p, se tiene que*

$$a^{p-1} \equiv 1 \text{ (mód } p).$$

Demostración. Sea a como en el teorema; mostraremos primero que el conjunto de números $a, 2a, 3a, \ldots, (p-1)a$ (mód p) es igual al conjunto $1, 2, 3, \ldots, (p-1)$ (mód p). En efecto, el conjunto $a, 2a, 3a, \ldots, (p-1)a$ contiene $(p-1)$ números y como $p \nmid a$, entonces ningún número de este conjunto es divisible por p. Supongamos ahora que tomamos dos de estos números ja y ka y que éstos son congruentes módulo p: $ja \equiv ka$ mód p. Entonces, $p|(j-k)a$ y como $p \nmid a$ entonces $p|j-k$. Pero como $1 \leq j, k \leq p-1$, entonces $|j-k| < p-1$. Notemos ahora que sólo hay un entero de valor absoluto menor que $p-1$ y divisible por p, a saber, el 0. Se sigue que $j = k$ y así los enteros $a, 2a, 3a, \ldots, (p-1)a$ son distintos mód p y como $1, 2, 3, \ldots, (p-1)$ son todos los enteros no cero distintos mód p, entonces los dos conjuntos anteriores son iguales. Se sigue que el producto, mód p, de los enteros de un conjunto es igual al producto, mód p, de los enteros del otro conjunto:

$$a(2a)(3a)\cdots(p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \text{ (mód } p),$$

por lo que agrupando los $(p-1)$ factores a del lado izquierdo obtenemos

$$a^{p-1}(p-1)! \equiv (p-1)! \text{ (mód } p),$$

donde observamos que el factorial $(p-1)!$ es coprimo con p y así lo podemos cancelar para obtener el pequeño teorema de Fermat $a^{p-1} \equiv 1$ (mód p). □

Leonhard Euler, matemático suizo, generalizó en el año 1750 el teorema de Fermat anterior a cualquier módulo m no necesariamente primo como sigue: para comenzar es fácil ver que el teorema de Fermat es falso si el exponente m no es primo, por ejemplo, si $m = 9$, tomando $a = 2$ se tiene que $2^{9-1} \equiv 4$ (mód 9), de tal forma que la pregunta que Euler tiene que responder es: ¿existe un exponente e, que dependa sólo del módulo m, tal que

$$(*) \qquad a^e \equiv 1 \text{ (mód } m)?$$

Observemos que si $a^e \equiv 1$ (mód m), entonces $a^e = 1 + mt$ y así $a^e - mt = 1$ por lo que a y m son coprimos. Esto sugiere que consideremos el conjunto

$$\{a \,:\, 1 \leq a \leq m \quad \text{y} \quad \text{mcd}(a, m) = 1\}.$$

Al cardinal de este conjunto se le denota $\phi(m)$ y a la función ϕ así definida se le llama la *función de Euler*. Por ejemplo, si $m = p$ es primo, se tiene que $\phi(p) = p - 1$. Y si $k \geq 1$ es cualquier entero y p es primo, para calcular $\phi(p^k)$ necesitamos contar los enteros entre 1 y p^k que sean coprimos con p^k. Para esto, basta contar aquellos enteros entre 1 y p^k que no son coprimos con p^k, *i.e.*, que son divisibles por p; pero esto último es fácil: los enteros entre 1 y p^k divisibles por p son:

$$p, 2p, 3p, 4p, \ldots, (p^{k-1} - 2)p, (p^{k-1} - 1)p, p^k$$

y hay p^{k-1} de ellos. Esto nos da la fórmula

$$\phi(p^k) = p^k - p^{k-1}.$$

Adicionalmente, se puede probar que la función ϕ de Euler es multiplicativa, es decir, $\phi(mn) = \phi(m)\phi(n)$ si $\text{mcd}(m, n) = 1$. Esto nos permite calcular $\phi(m)$ para cualquier entero $m \geq 1$. Para probar que ϕ es multiplicativa necesitaremos el resultado siguiente, que es el ejercicio 54, y como nos será también necesario para el algoritmo de encriptamiento que describiremos después, lo recordamos y demostramos a continuación: si a, b, c son tres enteros con a y b coprimos y tales que ambos dividen a c, entonces ab también divide a c. La demostración de esta afirmación es como sigue: ya que $a|c$ y $b|c$, entonces $c = aa'$ y $c = bb'$. Ahora, de $1 = as + bt$ (ya que a y b son coprimos), multiplicando por c se tiene que

$$c = acs + bct = abb's + baa't = ab(b's + a't),$$

por lo que $ab|c$ como se quería.

Mostraremos ahora que la función ϕ de Euler es multiplicativa: sean $m, n \geq 1$ dos enteros coprimos. Considere los conjuntos

$$A = \{a \in \mathbb{Z} \ : \ 1 \leq a \leq mn \quad \text{y} \quad \text{mcd}(a, mn) = 1\}$$

y

$$B = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 1 \leq a \leq m, \text{mcd}(a, m) = 1, 1 \leq b \leq n, \text{mcd}(b, n) = 1\}.$$

Observe que $A = (\mathbb{Z}/mn\mathbb{Z})^*$ tiene $\phi(mn)$ elementos y $B = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ y así, por el principio del producto, B tiene $\phi(m)\phi(n)$ elementos. Para probar la multiplicatividad de la función ϕ mostraremos que A y B

tienen la misma cardinalidad. Para esto, observe que si $a \in A = (\mathbb{Z}/mn\mathbb{Z})^*$ entonces $\text{mcd}(a, mn) = 1$ y por lo tanto $\text{mcd}(a, m) = 1 = \text{mcd}(a, n)$ ya que m y n dividen a mn. Se sigue que la correspondencia $F : A \to B$ dada por

$$F(a) := (a \text{ mód } m, a \text{ mód } n)$$

es una función.

(I) F es *inyectiva* ya que si $F(a) = F(b)$, entonces

$$(a \text{ mód } m, a \text{ mód } n) = (b \text{ mód } m, b \text{ mód } n)$$

por lo que $a \equiv b \pmod{m}$ y $a \equiv b \pmod{n}$ y como m y n son coprimos, por el ejercicio 54 que demostramos antes se sigue que $a \equiv b \pmod{mn}$, *i.e.*, $a = b$ en A como se quería.

(II) F es *suprayectiva* ya que si $(a \text{ mód } m, b \text{ mód } n)$ es cualquier elemento de $B = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, queremos encontrar un elemento $x \pmod{mn} \in A = (\mathbb{Z}/mn\mathbb{Z})^*$ tal que

$$(x \text{ mód } m, x \text{ mód } n) = (a \text{ mód } m, b \text{ mód } n),$$

es decir, x debe satisfacer las dos congruencias

$$x \equiv a \text{ mód } m$$
$$x \equiv b \text{ mód } n,$$

y una tal solución existe gracias al teorema chino del residuo, porque $\text{mcd}(m, n) = 1$.

Hemos así mostrado que $F : A \to B$ es biyectiva y por lo tanto A y B tienen el mismo número de elementos, es decir,

$$\phi(mn) = |A| = |B| = \phi(m)\phi(n),$$

como se quería.

La multiplicatividad de la función ϕ de Euler y el cálculo que hicimos antes de $\phi(p^k) = p^k - p^{k-1}$ para p un primo permiten calcular la función de Euler para cualquier entero $m \geq 1$, gracias al teorema fundamental de la aritmética:

EJERCICIO 79. Suponga que $p_1, p_2, \ldots, p_r$ son los primos distintos que dividen a m. Demuestre la siguiente fórmula para $\phi(m)$:

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Finalmente, la generalización de Euler del teorema de Fermat es:

TEOREMA III.38 (Euler). *Si* $\mcd(a, m) = 1$, *entonces* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración. Es una variación de la demostración del teorema de Fermat: sean $1 \leq b_1 < b_2 < \cdots < b_{\phi(m)} \leq m$ los $\phi(m)$ enteros entre 1 y m que son coprimos con m. Obsérvese que como $\mcd(a, m) = 1$ entonces el conjunto

$$b_1 a, b_2 a, \ldots, b_{\phi(m)} a \pmod{m}$$

es igual al conjunto

$$b_1, b_2, \ldots, b_{\phi(m)} \pmod{m}.$$

Una vez probado esto se consideran los correspondientes productos para obtener

$$a^{\phi(m)} b_1 b_2 \cdots b_{\phi(m)} \equiv b_1 b_2 \cdots b_{\phi(m)} \pmod{m}$$

y como $\mcd(b_j, m) = 1$ entonces $\mcd(b_1 b_2 \cdots b_{\phi(m)}, m) = 1$ por lo que este factor se puede cancelar de la congruencia anterior para obtener el teorema de Euler: $a^{\phi(m)} \equiv 1 \pmod{m}$. □

EJERCICIO 80. (1) Use el teorema pequeño de Fermat para:

(I) Encontrar un número $0 \leq a < 73$ tal que $a \equiv 9^{794} \pmod{73}$.

(II) Resolver la congruencia $x^{86} \equiv 6 \pmod{29}$.

(III) Resolver la congruencia $x^{39} \equiv 8 \pmod{13}$.

(2) En la demostración del pequeño teorema de Fermat apareció el número $(p-1)! \pmod{p}$, a pesar de que no nos hizo falta calcular su valor.

(I) Calcule $(p-1)! \pmod{p}$ para algunos valores pequeños del primo p, encuentre un patrón, haga una conjetura y demuéstrela.

(II) En las siguientes preguntas explique su respuesta:

- La congruencia $7^{1660565} \equiv 1 \pmod{1734251}$ es verdadera. ¿Puede de esto concluirse que el número 1734251 es compuesto?
- La congruencia $129^{64026} \equiv 1579 \pmod{64027}$ es verdadera. ¿Puede de esto concluirse que 64027 no es un primo?

(III) ¿Qué puede decir acerca de n si el valor de $\phi(n)$ es un primo?

(IV) ¿Qué puede decir de n si $\phi(n)$ es el cuadrado de un primo?

(V) Encuentre todos los valores de n para los cuales $\phi(n) = n/2$.

EJERCICIO 81. (1) Sean $b_1 < b_2 < \cdots < b_{\phi(m)}$ los enteros entre 1 y m que son coprimos con m y sea $B = b_1 b_2 \cdots b_{\phi(m)}$ su producto. El número B apareció en la demostración de la fórmula de Euler.

(I) Muestre que $B \equiv 1 \pmod{m}$ o $B \equiv -1 \pmod{m}$.

(II) Calcule B para algunos valores pequeños de m y trate de encontrar un patrón de cuándo es $+1 \pmod{m}$ y cuándo es $-1 \pmod{m}$.

(2) Explique por qué $\phi(m)$ siempre es par si $m \geq 3$.
(3) Observe que $\phi(m)$ casi siempre es divisible por 4. Describa todos los enteros m para los cuales $\phi(m)$ no es divisible por 4.
(4) Un número compuesto m se llama un *número de Carmichael* si la congruencia $a^{m-1} \equiv 1 \pmod{m}$ es verdadera para todos los enteros a tales que $\mcd(a, m) = 1$.

(I) Verifique que el entero $m = 561 = 3 \cdot 11 \cdot 17$ es un número de Carmichael. Notas: (1) No le estoy pidiendo que verifique la factorización de 561 que le di arriba. (2) Use el pequeño teorema de Fermat o el teorema de Euler para resolver este problema: no intente calcular las potencias $a^{m-1} \pmod{m}$ para todos los 320 posibles valores de a.

(II) Trate de encontrar otro número de Carmichael.

(III) ¿Cree que hay un número infinito de números de Carmichael?

Criptografía de clave pública. Desde tiempos remotos ha existido la necesidad de intercambiar información, y en ocasiones es deseable ocultar ésta para que sea accesible sólo al destinatario y evitar que sea leído por otras personas. Por ejemplo, en la época de los césares en Roma, el césar se comunicaba con sus generales encriptando sus mensajes por medio de una traslación del alfabeto, digamos recorriendo tres lugares las letras de tal forma que la A se convertía en D, la B en E, la C en F, y así sucesivamente hasta llegar a la V en Y, la W en Z, la X en A, la Y en B y la Z en C. El destinatario desencriptaba el mensaje haciendo la traslación inversa. Notemos que con este método, la persona que encripta el mensaje automáticamente puede desencriptarlo, tan sólo aplicando la inversa de la función que usó para encriptar. Por mucho tiempo se creyó que éste siempre sería el caso: con cualquier método de encriptamiento la persona que supiera cómo encriptar, automáticamente sabría cómo desencriptar.

Sin embargo, en las últimas décadas del siglo XX surgió la necesidad de tener un método de encriptamiento donde la persona o entidad que encriptara un mensaje no pudiera desencriptarlo si no tuviera a su alcance otros datos. Por ejemplo, un *banco* puede tener muchos *clientes* y entre los clientes y el banco se necesita intercambiar información, digamos transferencia de fondos, pagos, etc., y es necesario que esta información sólo pueda ser leída por el destinatario legítimo. Para esto, el banco y el cliente necesitan un método de encriptamiento para que el cliente pueda enviar instrucciones al banco y solamente el banco pueda leer el mensaje para ejecutar la instrucción, que puede ser algo tan común como un pago por tarjeta de crédito. Una forma eficiente de implementar tal sistema es el siguiente: el banco crea un sistema de encriptamiento donde una parte de las claves se hace pública y otra parte la retiene el banco como una clave privada. La idea es que con la clave pública los clientes pueden enviar mensajes encriptados al banco y a su vez el banco, con su clave privada o secreta es el único que puede desencriptar el mensaje. Nótese que como la clave de encriptamiento es pública se necesita que la persona o entidad que hace el encriptamiento no pueda a su vez desencriptar el mensaje sólo conociendo la clave pública. En otras palabras, se está pidiendo una función de encriptamiento con una *trampa* o dispositivo que haga improbable (extremadamente difícil) invertir la función tan sólo conociendo las claves públicas.

En esta sección describimos uno de los métodos más usados para implementar tal sistema de encriptamiento. El primer paso es convertir el mensaje

en una secuencia de números; una forma simple de hacerlo es asignarle un número de dos dígitos a cada letra del alfabeto, digamos de acuerdo con la tabla siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36	37

y al espacio entre palabras le asignamos los dígitos 99. Así, el mensaje "saludos a todos" se convierte en

S	A	L	U	D	O	S		A		T	O	D	O	S
30	11	22	32	14	26	30	99	11	99	31	26	14	26	30

es decir, se convierte en el número 301122321426309911993126142630.

Por supuesto que, en algún sentido, el mensaje ya está encriptado porque esta sucesión de dígitos esconde el mensaje original. Sin embargo, aun un criptoanalista no muy listo podría desencriptar este mensaje en unos cuantos minutos.

En 1976 W. Diffie y M. Hellman dieron una descripción teórica de un método de encriptamiento en el cual una parte sería pública, y en 1977 R. Rivest, A. Shamir y L. Adleman encontraron un esquema práctico para implementarlo. El método se conoce como el *criptosistema de clave pública* RSA. Las ideas involucradas son las siguientes: para encriptar un mensaje primero lo convertimos en una sucesión de dígitos (por ejemplo, como hicimos antes), lo cual nos da un número, que puede ser muy grande si el mensaje lo es. Previamente, la persona que desarrolla este criptosistema realiza lo siguiente:

(I) Elige dos números primos (grandes) p y q.

(II) Calcula el producto $m = pq$ como módulo.

(III) Calcula $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$.

(IV) Escoge un exponente entero e, coprimo con $\phi(m)$.

(v) Resuelve la congruencia $eu \equiv 1 \pmod{\phi(m)}$, notando que como e y $\phi(m)$ son coprimos, entonces la congruencia dada tiene solución. Denotemos con $u = d$ la solución positiva tal que $1 < d < \phi(m)$.

De todo lo anterior el encriptador hace públicos m y e pero mantiene p, q, $\phi(m)$ y d secretos. Así, la *clave pública* es el par $E = (m, e)$, por lo que quienquiera que desee enviarnos un mensaje encriptado usará sólo los valores públicos m, e y para encriptar su mensaje procede como sigue:

(1) Convierte su mensaje en una secuencia de dígitos como hicimos previamente.

(2) Usando el módulo m separa la secuencia de dígitos en bloques de números menores que m. Así, el mensaje se convierte ahora en una lista (ordenada) de bloques $a_1, a_2, \ldots, a_r$ (con cada $a_j < m$). Por supuesto que la elección de los bloques a_j no es única y sólo se pide que ningún bloque comience con cero, para evitar ambigüedades en el desencriptamiento.

(3) Usando el exponente e, calcula las potencias módulo m:

$$a_1^e \pmod{m}, a_2^e \pmod{m}, \ldots, a_r^e \pmod{m}$$

obteniendo así los números $b_j = a_j^e$ mód m y el mensaje encriptado que nos envía es la lista

$$b_1, b_2, \ldots, b_r.$$

¿Qué necesitamos para leer este mensaje? Es decir, ¿cómo recuperamos los números a_j de las congruencias $b_j \equiv a_j^e \pmod{m}$? En otras palabras, ¿cómo sacamos raíces e-ésimas módulo m, *i.e.*, cómo resolvemos las congruencias $x^e \equiv b_j \pmod{m}$?

Por supuesto que siempre se tiene el método crudo de substituir x por los enteros $0, 1, 2, \ldots, m-1$ hasta que encontremos la solución deseada. Sin embargo, si m es muy grande esto puede tomar mucho tiempo y no sería práctico. Resulta que, si conocemos $\phi(m)$ podemos calcular la raíz e-ésima de b_j módulo m fácilmente. En efecto, como $\mcd(e, \phi(m)) = 1$, la congruencia lineal

$$eu \equiv 1 \pmod{\phi(m)}$$

tiene soluciones y así podemos hallar un entero positivo $u = d$ que satisface esta congruencia (dicho en otras palabras, d es el inverso multiplicativo de e módulo $\phi(m)$). Afirmamos que la potencia

$$x_j := b_j^d \text{ (mód } m)$$

es una solución de la congruencia $x^e \equiv b_j$ (mód m). En efecto,

$$\begin{aligned} x_j^e &= (b_j^d)^e = b_j^{ed} \\ &= b_j^{1+\phi(m)v} \quad \text{ya que } ed = 1 + \phi(m)v \\ &= b_j (b_j^{\phi(m)})^v \\ &\equiv b_j \text{ (mód } m), \end{aligned}$$

donde en la última congruencia usamos el hecho de que

$$(*) \qquad b_j^{\phi(m)} \equiv 1 \text{ (mód } m), \qquad$$

la cual es cierta, por el teorema de Euler si $\text{mcd}(b_j, m) = 1$, pero esto último no necesariamente se cumple; sin embargo, b_j^d sigue siendo una raíz e-ésima de b_j aun cuando $\text{mcd}(b_j, m) > 1$ si m es producto de primos distintos, como es el caso en consideración. En efecto, como $m = pq$ con p, q primos distintos y como d satisface la congruencia $ed \equiv 1$ (mód $\phi(m)$), *i.e.*, satisface la ecuación diofantina $ed - \phi(m)v = 1$, con $\phi(m) = (p-1)(q-1)$, entonces

$$ed = 1 + \phi(m)v = 1 + (p-1)(q-1),$$

donde podemos suponer que $v > 0$. Para $x_j = b_j^d$, se tiene entonces que

$$\begin{aligned} x_j^e = (b_j^d)^e &= b_j^{ed} \\ &= b_j^{1+(p-1)(q-1)v} \\ &= b_j \left(b_j^{p-1}\right)^{(q-1)v}, \end{aligned}$$

donde observamos que, si $p | b_j$, entonces $b_j \equiv 0$ mód p y así

$$x_j^e = b_j \left(b_j^{p-1}\right)^{(q-1)v} \equiv 0 \equiv b_j \text{ mód } p,$$

y si $p \nmid b_j$, por el pequeño teorema de Fermat $b_j^{p-1} \equiv 1$ mód p, por lo que

$$x_j^e = b_j \left(b_j^{p-1}\right)^{(q-1)v} \equiv b_j(1) \equiv b_j \text{ mód } p.$$

En cualquiera de los dos casos se tiene que

$$x_j^e \equiv b_j \text{ mód } p.$$

De manera similar se prueba que

$$x_j^e \equiv b_j \text{ mód } q.$$

Hemos mostrado así que

$$p|(x_j^e - b_j) \qquad \text{y} \qquad q|(x_j^e - b_j)$$

con p, q primos distintos. Por el ejercicio (54) se sigue que $pq|(x_j^e - b_j)$, *i.e.*, $x_j^e \equiv b_j \text{ (mód } m)$, con $m = pq$.

Resumiendo, hemos probado que $x_j = b_j^d \text{ (mód } m)$ es tal que $x_j^e \equiv b_j \text{ (mód } m)$, con $0 < x_j < m$. Ahora, como $b_j = a_j^e \text{ (mód } m)$ por definición de b_j, entonces $a_j^e \equiv x_j^e \text{ (mód } m)$, y como $ed = 1 + \phi(m)v$, con $\phi(m) = (p-1)(q-1)$, entonces

$$(*) \qquad a_j a_j^{(p-1)(q-1)v} \equiv x_j x_j^{(p-1)(q-1)v} \text{ (mód } m).$$

Mostraremos ahora que $a_j \equiv x_j \text{ (mód } m)$. En efecto,

(I) Si $p|a_j$ y $q|a_j$, entonces $a_j \equiv 0 \text{ (mód } m)$ y así $0 \equiv a_j^{ed} \equiv x_j^{ed} \text{ (mód } m)$, por lo que $p|x_j$ y $q|x_j$, *i.e.*, $x_j \equiv 0 \text{ (mód } m)$ y consecuentemente

$$a_j \equiv 0 \equiv x_j \text{ (mód } m).$$

(II) Supongamos ahora que $p|a_j$ pero $q \nmid a_j$. Entonces $a_j^{q-1} \equiv 1 \text{ (mód } q)$ por el pequeño teorema de Fermat. Se sigue que

$$(1) \qquad \left(a_j^{q-1}\right)^{(p-1)v} \equiv 1 \text{ (mód } q).$$

Ahora, como $p|m$ y $m|(a_j^{ed} - x_j^{ed})$, entonces $p|(a_j^{ed} - x_j^{ed})$ y como además $p|a_j^{ed}$, se sigue que $p|x_j$. Observe entonces que q no puede dividir a x_j ya que de lo contrario se tendría que $x_j \equiv 0 \text{ (mód } m)$ y consecuentemente $x_j^{(p-1)(q-1)v} \equiv 0 \text{ (mód } m)$, de donde se obtendría que

$$a_j \equiv a_j a_j^{(p-1)(q-1)v} \equiv x_j x_j^{(p-1)(q-1)v} \equiv 0 \text{ (mód } m),$$

en contradicción con el hecho de que $q \nmid a_j$. Se sigue que $q \nmid x_j$ y por lo tanto $x_j^{(q-1)} \equiv 1 \pmod{q}$, por lo que

$$\left(x_j^{q-1}\right)^{(p-1)v} \equiv 1 \pmod{q}. \tag{2}$$

Note ahora que la congruencia $(*)$ sigue siendo válida módulo q. Así, de (1) y (2) se sigue que

$$a_j \equiv x_j \pmod{q}. \tag{3}$$

También, como $p|a_j$ y $p|x_j$, entonces $a_j \equiv 0 \equiv x_j \pmod{p}$, lo cual combinado con (3) implica que $a_j \equiv x_j \pmod{m}$, como se quería.

(III) Finalmente, si $p \nmid a_j$ y $q \nmid x_j$, usando el pequeño teorema de Fermat procediendo como en (II) se prueba que $a_j \equiv x_j \pmod{m}$ también.

Esto cubre todas las posibilidades y, finalmente, como ambos a_j y x_j están entre 0 y $m-1$, se sigue que $x_j = a_j$, *i.e.*, los números x_j recuperan los bloques originales, como se quería. Nótese que aquí está la razón por la cual elegimos los bloques $a_j < m$.

Usando el pequeño teorema de Fermat hemos podido recuperar los números $a_1, a_2, \ldots, a_r$ y por lo tanto ya desencriptamos el mensaje. Notemos que para hacer esto sólo necesitamos conocer $\phi(m)$ y podríamos pensar que esto lo podemos calcular de los datos públicos que incluyen a m. Sin embargo, si m es muy grande, $\phi(m)$ es difícil de calcular ya que, en nuestro caso $m = pq$ es el producto de dos primos (secretos) grandes y se tiene que

$$\phi(m) = (p-1)(q-1) = pq - p - q + 1 = m - p - q + 1,$$

y como m es público, para calcular $\phi(m)$ basta conocer $p+q$. Pero si esto fuera posible entonces ya conoceríamos a p y q ya que estos son raíces de la ecuación cuadrática

$$X^2 - (p+q)X + m = 0.$$

Es decir, para desencriptar un mensaje esencialmente se necesitan conocer los factores primos p y q de m. Si m no es muy grande una computadora sencilla lo puede factorizar, pero si m es muy grande (varios cientos de dígitos) hasta ahora no existe un algoritmo eficiente para factorizar a m, por lo que el método RSA descrito anteriormente es bastante seguro.

Ejemplo 15. El ejemplo siguiente, con primos pequeños para que los cálculos sean sencillos, está muy lejano de los ejemplos reales donde se usan primos grandes, y sólo es para mostrar cómo se implementa el método RSA. Supongamos que deseamos encriptar la palabra ALGO usando los primos $p = 11$, $q = 17$, el módulo $m = pq = 187$ (por lo que $\phi(m) = (11-1)(17-1) = 160$) y el exponente $e = 7$. Primero usamos la tabla que convierte letras en números y así obtenemos el número 11221726. Luego, separamos este número en bloques $a_j < 187$, digamos

$$a_1 = 112,\ a_2 = 21,\ a_3 = 7,\ a_4 = 26.$$

Después, calculamos

$$\begin{aligned} b_1 = a_1^e &= (112)^7 \equiv 73 \text{ (mód 187)} \\ b_2 = a_2^e &= (21)^7 \equiv 98 \text{ (mód 187)} \\ b_3 = a_3^e &= (7)^7 \equiv 182 \text{ (mód 187)} \\ b_4 = a_4^e &= (26)^7 \equiv 104 \text{ (mód 187)}, \end{aligned}$$

por lo que el mensaje encriptado es la secuencia de bloques:

$$73,\ 98,\ 182,\ 104.$$

Hagamos hincapié en que para encriptar el mensaje sólo se usaron los datos públicos m y e. Para desencriptar el mensaje anterior, necesitamos conocer $\phi(m)$ para resolver la congruencia

$$eu \equiv 1 \text{ mód } (\phi(m)),$$

que en nuestro ejemplo es

$$7u \equiv 1 \text{ (mód 160)},$$

de donde, usando los métodos correspondientes hallamos que $u = d = 23$ es una tal solución. Después, calculamos

$$\begin{aligned} x_1 = b_1^u &= (73)^{23} \equiv 112 \text{ (mód 187)} \\ x_2 = b_2^u &= (98)^{23} \equiv 21 \text{ (mód 187)} \\ x_3 = b_3^u &= (182)^{23} \equiv 7 \text{ (mód 187)} \\ x_4 = b_4^u &= (104)^{23} \equiv 26 \text{ (mód 187)}, \end{aligned}$$

y así, el mensaje desencriptado del ejemplo anterior es la secuencia de bloques:

$$112,\ 21,\ 7,\ 26,$$

i.e., el número 11221726, y usando la tabla que convierte letras en números, obtenemos el mensaje desencriptado: ALGO.

Aquí, el paciente lector ya ha notado la cantidad de cálculos involucrados, aun en este ejemplo con números pequeños. Para calcular estas potencias b^d hay un método muy sencillo que, en forma resumida, es usar *cuadrados sucesivos*. Para esto, notamos primero que podemos escribir el exponente d de la forma

$$d = c_n 2^n + c_{n-1} 2^{n-1} + \cdots + c_2 2^2 + c_1 2 + c_0$$

con los $c_j = 0$ o 1. Decimos que ésta es la *expansión binaria* de d y a veces escribimos

$$d = c_n c_{n-1} \cdots c_2 c_1 c_0.$$

Después, escribimos

$$b^d = (b^2)^{c_n 2^{n-1} + c_{n-1} 2^{n-2} + \cdots + c_2 2 + c_1} (b)^{c_0} \tag{1}$$

donde

$$b^{c_0} = \begin{cases} 1 & \text{si} \quad c_0 = 0 \\ b & \text{si} \quad c_0 = 1 \end{cases}$$

y observando que b^2 es fácil de calcular (reduciéndolo módulo m después). Poniendo $A_1 = b^{c_0} \pmod m$ la igualdad (1) queda

$$\begin{aligned} b^d &\equiv (b^2)^{c_n 2^{n-1} + c_{n-1} 2^{n-2} + \cdots + c_2 2 + c_1} A_1 \\ &\equiv (b^4)^{c_n 2^{n-2} + c_{n-1} 2^{n-3} + \cdots + c_3 2 + c_2} (b^2)^{c_1} A_1 \pmod m, \end{aligned}$$

y poniendo $A_2 = (b^2)^{c_1} A_1 \pmod m$, la última igualdad queda

$$b^u \equiv (b^8)^{c_n 2^{n-3} + c_{n-1} 2^{n-4} + \cdots + c_4 2 + c_3} (b^4)^{c_2} A_2 \pmod m.$$

Continuando de esta manera, se obtiene una sucesión de números

$$A_1, A_2, \ldots, A_n$$

donde $A_n \equiv b^d \pmod{m}$, como se quería. Éste fue el método que usamos para calcular las potencias en el ejemplo anterior. Aquí, la expansión binaria del exponente $d = 23$ es

$$23 = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0,$$

i.e., $23 = 10111$. Así, para calcular 182^{23} primero calculamos

$$\begin{aligned} 182^2 &\equiv 25 \pmod{187} \\ 182^4 \equiv 25^2 &\equiv 64 \pmod{187} \\ 182^8 \equiv 64^2 &\equiv 169 \pmod{187} \\ 182^{16} \equiv 169^2 &\equiv 137 \pmod{187} \end{aligned}$$

por lo que

$$182^{23} \equiv 182^{1\times 2^4+0\times 2^3+1\times 2^2+1\times 2^1+1\times 2^0} \equiv 137 \times 64 \times 25 \times 182 \equiv 7 \pmod{187}.$$

EJERCICIO 82. (1) Usando el módulo $m = pq = 319$ y el exponente $e = 3$, que es coprimo con $\phi(m) = 280$, encripte el mensaje SALUDOS A TODOS.

(2) Hace mucho, mucho tiempo, en una galaxia muy lejana, te encontrabas en una misión ultrasecreta llevando guardada en tu memoria las claves secretas $p = 23$ y $q = 29$ y el exponente $e = 5$. Al llegar al Hotel Casablanca donde te alojas, para descansar después de un día arduo de estudiar matemáticas, poco después de la medianoche alguien toca a tu puerta y un misterioso mensajero te deja un papel con el mensaje encriptado siguiente:

16 476 655 323 493 304 113 457

Tu misión, si la aceptas, está en el mensaje anterior.

Eficiencia de algunos algoritmos. A lo largo de este capítulo hemos encontrado varios algoritmos aritméticos, cuya importancia teórica es incuestionable, el algoritmo de la división (III.13), el algoritmo de Euclides (III.17) para calcular el máximo común divisor, la criba de Eratóstenes para encontrar enteros primos, algoritmos para resolver ecuaciones diofantinas lineales en dos variables y congruencias lineales en una variable, y el método de los cuadrados sucesivos para calcular potencias y raíces módulo n. Sin embargo, desde el punto de vista práctico, al implementar el criptosistema RSA, la eficiencia de los algoritmos anteriores es un tema importante que no hemos considerado hasta ahora y es el objetivo de los párrafos siguientes:

Eficiencia del algoritmo de Euclides. Cuando se tiene un algoritmo para hacer algo, uno también se pregunta por la eficiencia del algoritmo, es decir, ¿en cuántos pasos, a lo más, el algoritmo nos da el resultado buscado? Para el caso del algoritmo de Euclides, la pregunta es: ¿dados los enteros a, b, cuál es el máximo número de pasos necesarios para calcular $\mcd(a,b)$? Para comenzar, es claro que el residuo de las divisiones sucesivas del algoritmo de Euclides se vuelve 0 a lo más en $|b|$ pasos. Sin embargo, el algoritmo de Euclides es más eficiente que esto. En efecto, supongamos que $a \geq b > 0$ son enteros y consideremos las divisiones sucesivas:

$$\begin{aligned}
a &= bq_1 + r_1 && \text{con} && 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2 && \text{con} && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && \text{con} && 0 \leq r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4 && \text{con} && 0 \leq r_4 < r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} && \text{con} && 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n && \text{con} && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 && \text{con} && r_{n+1} = 0
\end{aligned}$$

por lo que $\mcd(a,b) = r_n$. Pongamos $r_0 := b$ y $r_{-1} = a$. Entonces,

$$r_{i+1} < \frac{1}{2} r_{i-1}.$$

Demostración. En efecto, al comparar r_i y $\frac{1}{2}r_{i-1}$, por tricotomía se tienen dos casos: $r_i \leq \frac{1}{2}r_{i-1}$ o $r_i > \frac{1}{2}r_{i-1}$. En el primer caso ya terminamos porque $r_{i+1} < r_i$. En el segundo caso, sabemos que $r_{i-1} = r_i q_i + r_{i+1}$ con $0 \leq r_{i+1} < r_i$ y, como estamos asumiendo que $r_i > \frac{1}{2}r_{i-1}$, entonces

$$(*) \qquad r_{i+1} = r_{i-1} - r_i q_i < r_{i-1} - \frac{1}{2} r_{i-1} q_i = r_{i-1}\left(1 - \frac{1}{2} q_i\right);$$

claramente $q_i \neq 0$ (ya que de lo contrario $r_{i+1} = r_{i-1}$, en contradicción con el hecho de que los r_j son estrictamente decrecientes). Se sigue que $q_i \geq 1$ y por lo tanto $(*)$ implica que

$$r_{i+1} < r_{i-1}\left(1 - \frac{1}{2} q_i\right) \leq r_{i-1}\left(1 - \frac{1}{2}\right) = \frac{1}{2} r_{i-1},$$

como se quería. □

Sea $\log_2(b)$ el logaritmo en base 2 del entero b, es decir, $\log_2 b = r \Leftrightarrow 2^r = b$.

PROPOSICIÓN III.39. *Sean $a \geq b > 0$ enteros. Entonces, el algoritmo de Euclides para calcular* $\mathrm{mcd}(a, b)$ *termina a lo más en* $2\log_2(b)$ *pasos, donde cada paso es una división con residuo.*

Demostración. Sean r_i los residuos de las divisiones sucesivas necesarias para obtener $r_n = \mathrm{mcd}(a, b)$ como antes. Mostraremos que $r_{2i} = 0$ para $2i \geq 2\log_2(b)$ (estamos asumiendo que $a \geq b$). En efecto, como $r_0 = b$, por lo demostrado antes del enunciado de la proposición, se tiene que $r_2 < \frac{1}{2}r_0$ y por lo tanto

$$r_2 < \frac{1}{2}r_0 = \frac{1}{2}b.$$

Se sigue que

$$r_4 < \frac{1}{2}r_2 < \frac{1}{4}b,$$

$$r_6 < \frac{1}{2}r_4 < \frac{1}{8}b,$$

$$r_8 < \frac{1}{2}r_6 < \frac{1}{16}b,$$

y, en general,

$$r_{2i} < \frac{1}{2^i}b.$$

Pero, como los r_{2i} son enteros ≥ 0, entonces tan pronto se tenga que $2^i \geq b$, se tendrá que $r_{2i} < 1$ y consecuentemente $r_{2i} = 0$. Ahora, aplicando $\log_2$ a $2^i \geq b$ se obtiene

$$i = i\log_2(2) = \log_2(2^i) \geq \log_2(b) \Rightarrow r_{2i} = 0,$$

es decir, $i \geq \log_2 b$ implica que $r_{2i} = 0$, *i.e.*, $2i \geq 2\log_2(b)$ implica que $r_{2i} = 0$, y por lo tanto el algoritmo de Euclides termina en a lo más $2\log_2(b)$ pasos. □

Eficiencia del cálculo de potencias y raíces mód n. Para encriptar o desencriptar un mensaje con el método RSA, además de resolver una ecuación diofantina lineal usando el algoritmo de Euclides, se tienen que calcular potencias a^k (mód n). Si uno tomara el enfoque directo, entonces primero se calcula $a^2 = a \cdot a$ y luego reduce módulo n, para obtener el número a_2;

después calcula $a_2 \cdot a$ y reduce módulo n, para obtener el número a_3, y así sucesivamente para al final, después de k operaciones obtener el número $a_k \equiv a_{k-1} \cdot a \equiv a^k \pmod{n}$, donde cada operación consiste de una multiplicación seguida de una reducción módulo n. Con este método se necesitan entonces n operaciones. El método de los *cuadrados sucesivos* que discutimos en la sección correspondiente es mucho más eficiente ya que para calcular $a^k \pmod{n}$, primero escribimos en notación binaria al entero k:

$$(*) \qquad k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + k_3 \cdot 2^3 + \cdots + k_t \cdot 2^t$$

donde cada k_j es 0 o 1. Después ponemos $A_0 := a$ y calculamos los números

$$A_1 := A_0^2, \quad A_2 := A_1^2, \quad \ldots, A_t := A_{t-1}^2,$$

y al mismo tiempo reducimos módulo n. Después, de estos A_i escogemos aquellos para los cuales los coeficientes k_i de $(*)$ son 1 y se tiene que a^k es el producto de estos A_i.

Observe que se necesitan t operaciones para obtener los a_i y se necesitan a lo más t operaciones para obtener a^k. Por lo tanto se requieren a lo más $2t$ operaciones para calcular $a^k \pmod{n}$. Note que el número de operaciones depende del tamaño de k y se tiene que

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \cdots + k_t \cdot 2^t \geq 2^t$$

y por lo tanto $t \leq \log_2(k)$. Hemos así probado:

PROPOSICIÓN III.40. *Sean a, k, n enteros positivos. Entonces, el método de los cuadrados sucesivos para calcular $a^k \pmod{n}$ termina a lo más en $2\log_2(k)$ pasos, donde cada paso es una multiplicación y una reducción módulo n.* □

Ejemplo 16. Para el exponente $k = 1000$, primero escribimos 1000 en base 2:

$$k = 1000 = 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 = 1111101000,$$

por lo que a^{1000} es:

$$a^{1000} = a^{2^9} \cdot a^{2^8} \cdot a^{2^7} \cdot a^{2^6} \cdot a^{2^5} \cdot a^{2^3}$$

y los números a^{2^j} se calculan poniendo $A_0 = a$:

$$\begin{aligned} A_1 &= A_0^2 \ (\text{mód } n) \\ A_2 &= A_1^2 \ (\text{mód } n) \\ A_3 &= A_2^2 \ (\text{mód } n) \\ &\vdots \\ A_9 &= A_8^2 \ (\text{mód } n) \end{aligned}$$

y finalmente

$$a^{1000} = A_9 \cdot A_8 \cdot A_7 \cdot A_6 \cdot A_5 \cdot A_3 \ (\text{mód } n),$$

por lo que se necesitan 9 operaciones para obtener los A_j y 6 operaciones para multiplicar estos A_j y así se requieren 15 operaciones para calcular a^{1000} lo cual es mucho mejor que las $k - 1000$ operaciones que se necesitarían para hacerlo directamente.

EJERCICIO 83. Discuta la eficiencia del algoritmo de la división.

EJERCICIO 84. Analice la eficiencia de la criba de Eratóstenes.

Firmas digitales. La criptografía de clave pública se usa, entre otras cosas, para que bancos y clientes intercambien información mediante computadoras, tales como transferencias de dinero y pagos de tarjetas, y es claro por qué la información que se envía por medios electrónicos debe estar encriptada.

Un problema que se presenta, y que hasta ahora no hemos considerado, es que como la clave de encriptamiento del banco es pública, cualquier persona puede enviar un mensaje encriptado con la clave pública pidiendo al banco, por ejemplo, que transfiera dinero de la cuenta de un cliente legítimo a la cuenta de la persona que envía el mensaje. ¿Cómo puede determinar el banco que el mensaje que recibió provino de un cliente legítimo?, es decir, ¿cómo puede firmarse un mensaje electrónico?

La respuesta es muy simple, funciona para cualquier criptosistema de clave pública y fue descrita en el artículo original donde se propuso el sistema RSA que discutimos anteriormente. Para explicarlo, recordemos que en el criptosistema RSA el banco tiene un par de primos p, q cuyo producto es el entero $m = pq$ y un exponente e coprimo con $\phi(m)$. El banco hace pública la clave $E = (e, m)$, calcula la inversa d de e módulo $\phi(m)$ y mantiene secreta su clave de desencriptamiento $D = (d, m)$. Recordemos que si un

cliente quiere enviar un mensaje encriptado con la clave pública del banco, después de convertir su mensaje en un número y separar éste en bloques $b < m$, encripta el bloque b con la receta

$$E(b) = \text{residuo de } b^e \text{ módulo } m$$

y el banco recibe el bloque encriptado $a \equiv b^e$ mód m. Para desencriptar este bloque el banco usa su clave privada y calcula

$$D(a) = \text{residuo de } a^d \text{ módulo } m.$$

Denotemos con E_B y D_B las claves públicas y privadas del banco B, y para el cliente C se desarrolla su propio sistema RSA de encriptamiento, con claves pública y privada E_C y D_C, respectivamente. Sea b un bloque del mensaje que el cliente C desea enviar (firmado) al banco B; para esto el cliente usa la clave pública E_B del banco B y calcula $E_B(b)$; sin embargo, en lugar de enviar el bloque $E_B(b)$ el cliente envía el bloque $E_B(D_C(b))$ encriptando primero el bloque b con su clave privada D_C y luego con la clave pública E_B del banco. ¿Cómo procede el banco para desencriptar el mensaje $E_B(D_C(b))$ y verificar al mismo tiempo la autenticidad de la firma del cliente? Muy fácil, el banco aplica su clave privada D_B y obtiene el bloque $D_C(b)$ ya que $D_B \circ E_B = \text{id}$; después, aplica la clave pública del cliente E_C para obtener $E_C(D_C(b)) = b$.

Observe que este método permite tener la seguridad de que el bloque b se originó del cliente C ya que si el bloque $E_C D_B(E_B D_C(b))$ tiene sentido, entonces como el banco aplicó la composición $E_C D_B$, el bloque b debió ser encriptado con la composición $E_B D_C$, donde D_C es la clave secreta del cliente C.

Hay un pequeño problema con el procedimiento anterior: si

$$E_B = (e_B, m_B) \quad \text{y} \quad E_C = (e_C, m_C)$$

son las claves públicas del banco y del cliente, respectivamente, y si b es un bloque del mensaje que el cliente desea enviar al banco, entonces para firmar el mensaje el cliente debe calcular $D_C(b)$ y para esto requiere que $b < m_C$; después debe calcular $E_B(D_C(b))$ y para esto requiere que $D_C(b) < m_B$; ahora, como no sabemos por adelantado que $D_C(b) < m_B$, debemos garantizar esto desde el principio y el procedimiento es como sigue: como m_B y m_C son públicos, podemos compararlos para saber cuál es el menor.

Por ejemplo, si sucede que $m_C < m_B$, encriptamos el bloque b usando la composición $E_B D_C$ ya que $D_C(b) < m_C < m_B$ y por lo tanto ya podemos aplicar E_B a $D_C(b)$. Por otra parte, si sucediera que $m_B < m_C$, entonces invertimos el orden de la composición y encriptamos el bloque b usando $D_C E_B$ ya que así, como $b < m_B < m_C$, entonces $E_B(b) < m_B < m_C$, por lo que podemos aplicar D_C a $E_B(b)$. En otras palabras, el mensaje siempre se puede firmar eligiendo los bloques b de tal forma que sean menores que m_B y m_C, y el cliente aplica las funciones D_C y E_B primero la que corresponda al valor m que sea el menor de m_B y m_C.

III.10 Bibliografía

[1] Adleman, L., R. L. Rivest, A. Shamir, "A method for obtaining digital signatures and public-key cryptosystems", *Comm. ACM* **21** (1978), 120-126.

[2] Coutinho, S. C., *The Mathematics of ciphers*, A. K. Peters, Wellesley (Massachusetts), 1999.

[3] Weil, A., *Number Theory: An approach through history from Hammurapi to Legendre*, Birkhäuser Verlag, Boston, 2001.

[4] Zaldívar, F., "El pequeño teorema de Fermat", *Misc. Mat.*, **34**, 2001, 73-84.

IV. EL CAMPO DE NÚMEROS RACIONALES

Los números enteros se pueden sumar, restar y multiplicar, pero en general no se puede hacer *divisiones* con ellos, por ejemplo $\frac{2}{5} \notin \mathbb{Z}$, es decir, no existe un número entero x tal que $5x = 2$. Para poder resolver ecuaciones tan simples como la anterior es necesario añadir al conjunto $\mathbb{Z}$ las *fracciones*. Los números así obtenidos se llaman *números racionales* (del latín *ratio*, razón o cociente). La idea de la construcción de estos nuevos números es pensar a cada racional como un cociente de enteros, *i.e.,* como $\frac{m}{n}$ con $m, n \in \mathbb{Z}$ y con $n \neq 0$. Ahora, como en $\mathbb{Z}$ en general no se puede dividir, entonces pensaremos a $\frac{m}{n}$ como a un par ordenado $(m, n) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Así, dados dos pares ordenados $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$, si pensamos al par (a, b) como a/b y al par (c, d) como c/d y si queremos que sean iguales, *i.e.*, que $a/b = c/d$, como no hay división en $\mathbb{Z}$, entonces mejor escribimos la igualdad anterior como $ad = bc$ donde involucramos sólo operaciones permitidas en $\mathbb{Z}$. Con esta idea como motivación se introduce la relación siguiente en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$:

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc.$$

Lema IV.1. *La relación anterior es una relación de equivalencia en* $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.

Demostración. Sólo probaremos la transitividad y para esto supongamos que $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$. Entonces $ad = bc$ y $cf = de$. Multiplicando por f la primera igualdad y por b la segunda igualdad se tiene que: $adf = bcf$ y $bcf = bde$, de donde se sigue que $adf = bde$ y como $d \neq 0$, cancelando d de esta última igualdad se sigue $af = be$, *i.e.,* $(a, b) \sim (e, f)$. □

Ejercicio 1. Demuestre la reflexividad y simetría.

El conjunto cociente $\mathbb{Z} \times (\mathbb{Z} - \{0\}) / \sim$ se denota $\mathbb{Q}$ y a sus elementos, que son clases de equivalencia de pares ordenados (a, s) con $a \in \mathbb{Z}$ y $s \in \mathbb{Z} - \{0\}$, se les llama *números racionales* y los denotamos mediante $[a, s]$ o $\frac{a}{s}$.

IV.1 Operaciones en $\mathbb{Q}$

En el conjunto cociente $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$ se tienen operaciones de suma y producto de racionales definidas como sigue: sean $[a, s], [b, t] \in \mathbb{Q}$ y escojamos representantes $(a, s) \in [a, s]$ y $(b, t) \in [b, t]$:

Suma. Una vez elegidos los representantes anteriores se "suman" como sigue:

$$(a, s) + (b, t) := (at + bs, st)$$

y luego se toma la clase de equivalencia $[at + bs, st] \in \mathbb{Q}$. Por supuesto que hay que probar que esta "definición" no depende de la elección de los representantes en cada clase. Esto se hará en la primera parte del siguiente lema.

Producto. Con los representantes anteriores se define

$$(a, s)(b, t) := (ab, st)$$

observando que como $s \neq 0$ y $t \neq 0$, entonces $st \neq 0$ en $\mathbb{Z}$; después se toma la clase de equivalencia $[ab, st] \in \mathbb{Q}$. Que ésta es una buena definición es el contenido de la segunda parte del lema siguiente:

Lema IV.2. *Si* $(a, s) \sim (a', s')$ *y* $(b, t) \sim (b', t')$, *entonces:*

(1) $(at + bs, st) \sim (a't' + b's', s't')$.

(2) $(ab, st) \sim (a'b', s't')$.

Demostración. (1) Por hipótesis $as' = a's$ y $bt' = b't$. Entonces

$$\begin{aligned}(at + bs)s't' &= as'tt' + bss't' \\ &= a'stt' + b'ss't \quad \text{usando las hipótesis} \\ &= (a't' + b's')st.\end{aligned}$$

(2) Similarmente:

$$\begin{aligned}abs't' &= a'bst' \quad \text{usando la primera hipótesis} \\ &= a'b'st \quad \text{usando la segunda hipótesis.}\end{aligned}$$

□

Se tienen así las operaciones de suma y producto en $\mathbb{Q}$:

$$[a, s] + [b, t] = [at + bs, st]$$

y

$$[a, s][b, t] = [ab, st],$$

las cuales son las que uno ya conoce en la notación familiar de fracciones $\frac{m}{n}$.

Para mostrar que con estas operaciones $(\mathbb{Q}, +, \cdot)$ es un campo, necesitaremos los resultados siguientes:

LEMA IV.3. (1) $(a, s) \sim (0, t)$ *si y sólo si* $a = 0$.

(2) $\forall s \in \mathbb{Z} - \{0\}$ *se tiene que* $(s, s) \sim (1, 1)$.

Demostración. (1) ($\Rightarrow$): $(a, s) \sim (0, t) \Rightarrow at = s \cdot 0 = 0$ con $t \neq 0$ y como $\mathbb{Z}$ es dominio entero, entonces $a = 0$.

($\Leftarrow$): Si $a = 0$ entonces claramente $(0, s) \sim (0, t)$ ya que $0 \cdot t = 0 = s \cdot 0$.

(2) $\forall s \neq 0$ en $\mathbb{Z}$ se tiene que $s \cdot 1 = s = 1 \cdot s$ por lo que $(s, s) \sim (1, 1)$. □

Recordemos, del capítulo III, §III.6, que un *campo* K es un anillo conmutativo con 1, en el cual $1 \neq 0$ y tal que todos los elementos distintos de 0 de K tienen inverso multiplicativo.

EJERCICIO 2. Demuestre que todo campo es un dominio entero.

TEOREMA IV.4. *Con las operaciones anteriores* $(\mathbb{Q}, +, \cdot)$ *es un campo.*

Demostración. Ya hemos visto que $\mathbb{Q}$ es cerrado con respecto a las operaciones anteriores. Que la suma es asociativa y conmutativa lo dejamos como un ejercicio. El neutro aditivo de $\mathbb{Q}$ es la clase $[0, s]$ ya que para cualquier otro $[a, t] \in \mathbb{Q}$ se tiene que:

$$[a, t] + [0, s] = [as + 0 \cdot t, ts] = [as, ts] = [a, t],$$

la última igualdad porque $(as, ts) \sim (a, t)$. Denotaremos a la clase $[0, s] =: 0$.

El inverso aditivo de $[a, s] \in \mathbb{Q}$ es $[-a, s]$ ya que

$$[a, s] + [-a, s] = [as + (-a)s, ss] = [as - as, s^2] = [0, s^2] = 0.$$

Denotaremos al inverso aditivo de $[a, s]$ como $-[a, s]$.

Que el producto es asociativo, conmutativo y distribuye a la suma lo dejamos como ejercicio. El neutro multiplicativo de $\mathbb{Q}$ es la clase $[s, s]$ para cualquier $s \in \mathbb{Z} - \{0\}$ ya que para cualquier $[a, t] \in \mathbb{Q}$:

$$[a, t][s, s] = [as, ts] = [a, t].$$

Denotaremos a la clase $[s, s] =: 1$.

Si $[a,s] \neq 0$, por el lema anterior $a \neq 0$ en $\mathbb{Z}$ y por lo tanto $[s,a] \in \mathbb{Q}$ y el inverso multiplicativo de $[a,s] \neq 0$ es $[s,a]$ ya que $[a,s][s,a] = [as,sa] = [1,1] = 1$. Denotaremos al inverso multiplicativo de $[a,s]$ como $[a,s]^{-1}$. □

EJERCICIO 3. Demuestre la asociatividad y conmutatividad de la suma en $\mathbb{Q}$.

EJERCICIO 4. Demuestre la asociatividad y conmutatividad del producto en $\mathbb{Q}$.

EJERCICIO 5. Demuestre que el producto distribuye a la suma en $\mathbb{Q}$.

Observación. Como todos los elementos $\neq 0$ de $\mathbb{Q}$ tienen inverso multiplicativo, se puede definir la división en $\mathbb{Q}$ como sigue: sean $\alpha, \beta \in \mathbb{Q}$ con $\beta \neq 0$ (por lo que $\beta^{-1} \in \mathbb{Q}$). Se define

$$\frac{\alpha}{\beta} := \alpha \cdot \beta^{-1} \in \mathbb{Q}.$$

Así como los naturales se incluyen en el anillo $\mathbb{Z}$, veremos que $\mathbb{Z}$ se incluye en el campo $\mathbb{Q}$:

PROPOSICIÓN IV.5. *La función $\phi : \mathbb{Z} \to \mathbb{Q}$ definida mediante $\phi(m) := [m,1]$ es inyectiva y preserva las operaciones de $\mathbb{Z}$ y $\mathbb{Q}$, es decir:*

(1) $\phi(m+n) = \phi(m) + \phi(n)$.

(2) $\phi(mn) = \phi(m)\phi(n)$.

Nótese que en estas igualdades la suma y producto en los lados izquierdos son los de $\mathbb{Z}$ y los del lado derecho son los de $\mathbb{Q}$.

Demostración. Si $\phi(m) = \phi(n)$, entonces $[m,1] = [n,1]$ y así $(m,1) \sim (n,1)$ por lo que $m \cdot 1 = 1 \cdot n$, *i.e.*, $m = n$, *i.e.*, ϕ es inyectiva.

(1) $\phi(m+n) = [m+n,1] = [m,1] + [n,1] = \phi(m) + \phi(n)$.

(2) $\phi(mn) = [mn,1] = [m,1][n,1] = \phi(m)\phi(n)$. □

EJERCICIO 6. Demuestre que $\phi(0) = 0$ y que $\phi(1) = 1$, donde en los lados izquierdos el 0 y el 1 son los de $\mathbb{Z}$ y en los lados derechos son los de $\mathbb{Q}$.

Gracias a este ejercicio no hay confusión al denotar con los mismos símbolos a los ceros y unos de $\mathbb{Z}$ y de $\mathbb{Q}$.

EJERCICIO 7. Demuestre que para todo $a \in \mathbb{Z}$ se tiene que $\phi(-a) = -\phi(a)$.

La función inyectiva anterior $\phi : \mathbb{Z} \to \mathbb{Q}$ identifica a $\mathbb{Z}$ con su imagen en $\mathbb{Q}$ y así cada entero $m \in \mathbb{Z}$ lo podemos ver como un racional $m = [m, 1] \in \mathbb{Q}$.

COROLARIO IV.6. *Si $[a, s] \in \mathbb{Q}$, consideremos los enteros $a = [a, 1]$ y $s = [s, 1]$ vistos en $\mathbb{Q}$. Como $s \neq 0$ en $\mathbb{Z}$ entonces $[s, 1] \neq 0$ en $\mathbb{Q}$ y se tiene que*

$$[a, s] = \frac{a}{s} = as^{-1}.$$

Demostración.

$$as^{-1} = [a, 1][s, 1]^{-1} = [a, 1][1, s] = [a \cdot 1, 1 \cdot s] = [a, s]. \qquad \square$$

Este corolario justifica, *a posteriori*, el pensar al racional $[a, s]$ como a la *fracción* a/s.

IV.2 El orden en $\mathbb{Q}$

Para introducir una relación de orden en $\mathbb{Q}$ compatible con sus operaciones aritméticas, necesitamos definir una *clase positiva* $\mathbb{Q}^+$ en $\mathbb{Q}$, es decir, necesitamos identificar cuáles racionales a/b llamaremos positivos. La idea es simple, como $a, b \in \mathbb{Z}$, para que a/b sea positivo se requiere que a y b tengan el mismo signo, o lo que es lo mismo, se requiere que $ab > 0$ en $\mathbb{Z}$. Como a/b es una clase de equivalencia, debemos probar que lo anterior no depende del representante que se elija:

LEMA IV.7. *Si $(a, b) \sim (c, d)$ son representantes del mismo racional, entonces $ab > 0 \Leftrightarrow cd > 0$.*

Demostración. Supongamos que $ab > 0$. Como $(a, b) \sim (c, d)$, entonces $ad = bc$ y multiplicando esta igualdad por ad se tiene que $a^2d^2 = abcd$ donde observamos que $ab > 0$ implica que $a \neq 0$ y así $c \neq 0$ también. En la igualdad $a^2d^2 = (ab)(cd)$ se tiene entonces que $a^2 > 0$, $d^2 > 0$, $ab > 0$, por lo que $cd > 0$.

La implicación recíproca es similar. $\square$

Podemos entonces definir:

$$\mathbb{Q}^+ := \{[a, b] \in \mathbb{Q} \ : \ \forall (a, b) \in [a, b] \text{ se tiene que } ab > 0\}.$$

LEMA IV.8. *$\mathbb{Q}^+$ es una clase positiva en $\mathbb{Q}$, es decir,*

(1) *$\mathbb{Q}^+$ es cerrado bajo sumas y productos.*

(2) (Tricotomía): *Sea $a \in \mathbb{Q}$. Entonces se cumple una y sólo una de las afirmaciones siguientes:*

(I) $a \in \mathbb{Q}^+$.

(II) $-a \in \mathbb{Q}^+$.

(III) $a = 0$.

Demostración. (1) Si $[a,b],[c,d] \in \mathbb{Q}^+$ entonces $ab > 0$ y $cd > 0$ y así, en la suma $[a,b] + [c,d] = [ad + bc, bd]$ se tiene que

$$(ad + bc)(bd) = (ab)d^2 + b^2(cd)$$

donde $ab > 0, d^2 > 0, b^2 > 0, cd > 0$ en $\mathbb{Z}$, por lo que $(ab)d^2 + b^2(cd) > 0$.

En el producto $[a,b][c,d] = [ac, bd]$ se tiene que

$$(ac)(bd) = (ab)(cd) > 0.$$

(2) (Tricotomía): Sea $[a,b] \in \mathbb{Q}$ y supongamos que $[a,b] \neq 0$. entonces $ab \neq 0$ en $\mathbb{Z}$ y así, por tricotomía en $\mathbb{Z}$ se tiene que $ab > 0$ o $ab < 0$. Si $ab > 0$ entonces $[a,b] \in \mathbb{Q}^+$. Si $ab < 0$ en $\mathbb{Z}$ entonces $-(ab) = (-a)b > 0$ y así $-[a,b] = [-a,b] \in \mathbb{Q}^+$. □

Observación. Es claro que $1 = [s,s] \in \mathbb{Q}^+$.

Usando la clase positiva $\mathbb{Q}^+$ de $\mathbb{Q}$ se define la relación de orden siguiente: si $\alpha, \beta \in \mathbb{Q}$, diremos que $\alpha < \beta$ si $\beta - \alpha \in \mathbb{Q}^+$. Si $\alpha < \beta$ también lo denotamos mediante $\beta > \alpha$. Nótese que $\gamma > 0$ en $\mathbb{Q}$ quiere decir que $\gamma \in \mathbb{Q}^+$.

TEOREMA IV.9. *La relación $<$ de $\mathbb{Q}$ satisface:*

(1) *$<$ es transitiva, i.e., $a < b$ y $b < c$ implican que $a < c$.*

(2) *Compatibilidad con la suma: $a < b$ y $c \in \mathbb{Q}$ implican que $a + c < b + c$.*

(3) *Compatibilidad con el producto:*

(I) $a < b$ y $c > 0 \Rightarrow ac < bc$.

(II) $a < b$ y $c < 0 \Rightarrow ac > bc$.

(4) *Si* $a > 0$ *entonces* $a^{-1} > 0$.

(5) *Si* $0 < a < b$ *entonces* $0 < b^{-1} < a^{-1}$.

(6) *Si* $a \neq 0$ *en* $\mathbb{Q}$, *entonces* $a^2 > 0$.

Demostración. Las propiedades (1), (2) y (3) se demuestran como en el caso de $\mathbb{Z}$ y se dejan como ejercicio.

Para (4), como $a > 0$, por tricotomía no se puede tener que $a = 0$ así que $a \neq 0$ por lo que $a^{-1} \in \mathbb{Q}$ y $a^{-1} \neq 0$. Ahora, si sucediera que $a^{-1} < 0$, como $a > 0$ por la parte (3)(i) se tendría que $1 = aa^{-1} < 0$ en contradicción con el hecho de que $1 \in \mathbb{Q}^+$. Se sigue que $a^{-1} > 0$ como se quería.

Para (5), multiplicando las desigualdades $0 < a < b$ por $b^{-1} > 0$ (es positivo por la parte (4)) se obtiene que $0 < ab^{-1} < bb^{-1} = 1$ y multiplicando ahora esta desigualdad por $a^{-1} > 0$ (es positivo por (4)) se sigue que $0 < a^{-1}ab^{-1} < a^{-1}$, *i.e.*, $0 < b^{-1} < a^{-1}$.

Para (6), por tricotomía, $a > 0$ o $a < 0$. Si $a > 0$ entonces $a \in \mathbb{Q}^+$ por lo que $a^2 = aa \in \mathbb{Q}^+$, *i.e.*, $a^2 > 0$. Si $a < 0$ entonces $-a > 0$ y así $a^2 = (-a)(-a) \in \mathbb{Q}^+$ por lo que $a^2 > 0$. □

EJERCICIO 8. Demuestre las propiedades (1), (2) y (3) del teorema anterior.

EJERCICIO 9. Demuestre que $a < b$ y $c < d$ en $\mathbb{Q}$, entonces $a + c < b + d$.

A diferencia del anillo de los números enteros $\mathbb{Z}$, el campo de los números racionales $\mathbb{Q}$ es *denso*:

PROPOSICIÓN IV.10. *Si* $a, b \in \mathbb{Q}$ *y* $a < b$, *entonces existe otro racional* $c \in \mathbb{Q}$ *tal que* $a < c < b$.

Demostración. Mostraremos que $c := \frac{1}{2}(a + b) \in \mathbb{Q}$ sirve. En efecto,

$$\begin{aligned} a < b &\Rightarrow 2a = a + a < a + b \\ &\Rightarrow a < \frac{1}{2}(a + b) \end{aligned}$$

y

$$\begin{aligned} a < b &\Rightarrow a + b < b + b = 2b \\ &\Rightarrow \frac{1}{2}(a + b) < b \end{aligned}$$

y de las dos desigualdades anteriores se sigue que $a < \frac{1}{2}(a + b) < b$. □

Dados racionales $\alpha, \beta \in \mathbb{Q}$, diremos que $\alpha \leq \beta$ si $\alpha < \beta$ o $\alpha = \beta$.

EJERCICIO 10. La relación $\leq$ es una relación reflexiva, antisimétrica y transitiva en $\mathbb{Q}$.

EJERCICIO 11. Si $a < b$ y $b \leq c$, demuestre que $a < c$.

TEOREMA IV.11 (Propiedad arquimediana de $\mathbb{Q}$). *Si $a, b \in \mathbb{Q}$ son tales que $0 < a < b$, entonces existe $n \in \mathbb{N}$ tal que $na > b$.*

Demostración. Como $b > 0$ por (IV.9)(4) se tiene que $b^{-1} > 0$ y así $\frac{a}{b} = ab^{-1} > 0$. Por densidad (IV.10) existe otro racional $m/n \in \mathbb{Q}$ tal que $\frac{a}{b} > \frac{m}{n} > 0$, y como $m/n \in \mathbb{Q}^+$ entonces podemos escoger $m, n \in \mathbb{N}$ y así $na > mb$. Ahora, como $m \geq 1$ y como $b > 0$ entonces $mb \geq 1 \cdot b = b$. Se sigue que $na > mb \geq b$ por lo que $na > b$. □

EJERCICIO 12. Si $a \in \mathbb{Q}$ demuestre que existe $n \in \mathbb{N}$ tal que $a < n$.

Valor absoluto en $\mathbb{Q}$. Si $a \in \mathbb{Q}$, se define su valor absoluto $|a|$ como:

$$|a| := \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0. \end{cases}$$

EJERCICIO 13. Si $a \in \mathbb{Q}$, demuestre que $|a| = |-a|$.

PROPOSICIÓN IV.12. *El valor absoluto es una función $|\ |_1 : \mathbb{Q} \to \mathbb{Q}^+ \cup \{0\}$ que satisface las propiedades siguientes:*

(1) $\forall a \in \mathbb{Q}$ *se tiene que* $|a| \geq 0$ *y más aún,* $|a| = 0 \Leftrightarrow a = 0$.

(2) $\forall a \in \mathbb{Q}$ *se tiene que* $\pm a \leq |a|$.

(3) $|ab| = |a||b|$ $\forall a, b \in \mathbb{Q}$.

(4) $|a + b| \leq |a| + |b|$ $\forall a, b \in \mathbb{Q}$ *(desigualdad del triángulo).*

(5) $||a| - |b|| \leq |a - b|$ $\forall a, b \in \mathbb{Q}$.

Demostración. La afirmación inicial y la parte (1) las dejamos como un ejercicio. Para (2), si $a \geq 0$ entonces $a = |a|$ y si $a < 0$ entonces $-a > 0$ y como $|a| > 0$ por la parte (1), se sigue que $|a| + (-a) \in \mathbb{Q}_+$ y por lo tanto $|a| > a$.

Para (3) consideremos los casos:

(I) $a \geq 0$ y $b \geq 0$ y por lo tanto $ab \geq 0$, por lo que $|ab| = ab$, $|a| = a$, $|b| = b$ y así $|ab| = ab = |a||b|$.

(II) $a < 0$ y $b < 0$ y por lo tanto $-a > 0$ y $-b > 0$ por lo que $ab = (-a)(-b) > 0$ y así $|ab| = ab = (-a)(-b) = |a||b|$.

(III) $a \geq 0$ y $b < 0$ y por lo tanto $ab \leq 0$ y así $|ab| = -(ab) = a(-b) = |a||b|$.

(IV) El caso $a < 0$ y $b \geq 0$ es similar al anterior.

Para (4) consideremos los casos:

(I) Si $a + b \geq 0$ entonces $|a + b| = a + b \leq |a| + |b|$, la desigualdad por la parte (2).

(II) Si $a + b < 0$ entonces $|a + b| = -(a + b) = -a - b \leq |a| + |b|$, la desigualdad por la parte (2).

(5) Escribiendo $a = (a - b) + b$, por la desigualdad del triángulo se tiene que:

$$|a| = |(a - b) + b| \leq |a - b| + |b|$$

por lo que

$$|a| - |b| \leq |a - b|. \tag{1}$$

Similarmente, escribiendo $b = a - (a - b)$ se sigue que $|b| - |a| \leq |a - b|$, *i.e.*,

$$-(|a| - |b|) = |b| - |a| \leq |a - b|. \tag{2}$$

De (1) y (2) y por definición del valor absoluto se sigue que

$$||a| - |b|| \leq |a - b|. \qquad \square$$

EJERCICIO 14. Demuestre la afirmación inicial y la parte (1) de la proposición anterior.

EJERCICIO 15. Demuestre que para todo $a, b \in \mathbb{Q}$ se tiene que $|a \cdot b| \leq |a| + |b|$.

EJERCICIO 16. Por inducción sobre n demuestre que si $a_1, \ldots, a_n \in \mathbb{Q}$, entonces $|a_1 + \cdots + a_n| \leq |a_1| + \cdots + |a_n|$.

EJERCICIO 17. Sea $\mathbb{Q}^+$ el subconjunto de racionales positivos. Demuestre que $\mathbb{Q}^+$ no tiene elemento menor, *i.e.*, el principio del buen orden no es válido en $\mathbb{Q}$.

EJERCICIO 18. Si $a < b$ en $\mathbb{Q}$, demuestre que existen infinitos $x \in \mathbb{Q}$ tales que $a < x < b$.

EJERCICIO 19. Si $a, b, c, d \in \mathbb{Q}$, demuestre que

$$|ac + bd| \leq \sqrt{(a^2 + b^2)(c^2 + d^2)}.$$

V. EL CAMPO DE NÚMEROS REALES

Los números racionales los podemos sumar, restar, multiplicar y dividir (excepto por 0) pero hay algunas operaciones naturales que, en general, no son cerradas en $\mathbb{Q}$. Veamos un ejemplo: si $\alpha \in \mathbb{Q}$ podemos pensar en *la raíz cuadrada* de α, es decir, considerar a otro número β cuyo cuadrado sea α, *i.e.*, $\beta^2 = \alpha$. Por ejemplo, para el $9 \in \mathbb{Q}$ se tiene que $3^2 = 9$. Como es usual denotamos a $3 = \sqrt{9}$ y en general a $\beta = \sqrt{\alpha}$. Notemos ahora que si $p \in \mathbb{Z} \subseteq \mathbb{Q}$ es un entero primo (positivo), *no existe un número racional* $a/b \in \mathbb{Q}$ *tal que* $\sqrt{p} = a/b \in \mathbb{Q}$; es decir, $\sqrt{p} \notin \mathbb{Q}$. En efecto, supongamos por un momento que $\sqrt{p} \in \mathbb{Q}$ y escribamos $\sqrt{p} = a/b$ con $a, b \in \mathbb{Z}$. Simplificando esta fracción si hiciera falta podemos suponer que $\text{mcd}(a, b) = 1$. Entonces elevando al cuadrado la igualdad $\sqrt{p} = a/b$ obtenemos que $p = a^2/b^2$ y así $a^2 = pb^2$ en $\mathbb{Z}$, por lo que $p|a^2 = aa$, y como p es primo se sigue que $p|a$; se tiene entonces que $a = pt$ con $t \in \mathbb{Z}$, y substituyendo en la ecuación $a^2 = pb^2$ se obtiene que $p^2t^2 = pb^2$, de donde cancelando p se sigue que $pt^2 = b^2$, por lo que $p|b^2 = bb$, y como p es primo esto implica que $p|b$. Hemos mostrado así que $p|a$ y $p|b$, en contradicción con la suposición inicial de que $\text{mcd}(a, b) = 1$. Se sigue que $\sqrt{p} \notin \mathbb{Q}$. Es decir, no existe un racional $x \in \mathbb{Q}$ tal que $x^2 = p$. De alguna forma tenemos que añadir nuevos números a $\mathbb{Q}$ para incluir a raíces cuadradas como la anterior y muchos otros números que se obtienen por medio de operaciones sencillas con números racionales.

Ejercicio 1. Si $n \geq 2$ es entero y $p \in \mathbb{Z}$ es primo positivo, demuestre que $\sqrt[n]{p} \notin \mathbb{Q}$.

Consideremos ahora el ejemplo, cuando $p = 2$, $\sqrt{2} \notin \mathbb{Q}$ y observemos que $1 < \sqrt{2} < 2$. De hecho, unos cálculos sencillos muestran que:

$$1 < \sqrt{2} < 2$$
$$1.4 < \sqrt{2} < 1.42$$
$$1.41 < \sqrt{2} < 1.415$$
$$1.4114 < \sqrt{2} < 1.4143,$$

etcétera, donde los números a la izquierda y derecha de $\sqrt{2}$ son racionales, por ejemplo, $1.42 = 142/100$. Este ejemplo sugiere que el número $\sqrt{2}$ se puede aproximar mediante números racionales a_n de tal manera que la diferencia entre $\sqrt{2}$ y a_n sea arbitrariamente pequeña. Los números racionales a_n se pueden elegir uno por cada natural $n \in \mathbb{N}$, de tal forma que cuando n crece los números a_n se acercan a $\sqrt{2}$. Estas ideas se formalizan como sigue.

V.1 Sucesiones en $\mathbb{Q}$

Al elegir un (único) número racional a_n para cada natural $n \in \mathbb{N}$ se tiene una función $a : \mathbb{N} \to \mathbb{Q}$ a la que se llama una *sucesión de números racionales.* Se suele usar la notación $a(n) =: a_n$ para denotar al valor de a en n y algunas veces escribiremos a esta función como $\{a_n\}$ o (a_n) para indicar que se tiene una sucesión con valores $a_n \in \mathbb{Q}$. A veces también se usa la notación $a_1, a_2, a_3, \ldots$

Ejemplo 1. Si $a \in \mathbb{Q}$ es fijo, la sucesión $a_n = a$ (para todo $n \in \mathbb{N}$) se llama la *sucesión constante* de valor a.

Ejemplo 2. La sucesión $a_n = n$ se llama la sucesión idéntidad.

Ejemplo 3. Para $n \in \mathbb{N}$, como $\frac{3n}{2n+1} \in \mathbb{Q}$, se tiene la sucesión de racionales

$$\left\{ \frac{3n}{2n+1} \right\}$$

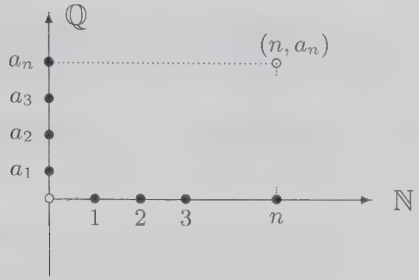
.

Ejemplo 4. Considere números racionales a_n definidos recursivamente como sigue:

$$a_1 = 1 \text{ y } a_{n+1} := \frac{a_n^2 + 2}{2a_n}. \text{ Por ejemplo, } a_2 = 3/2,\ a_3 = 17/12.$$

¿Podría calcular los primeros 10 términos de esta sucesión, en decimales?

Uno puede visualizar una sucesión de racionales poniendo en un eje horizontal al dominio de la sucesión, *i.e.*, a los números naturales y en un eje vertical a los números racionales, de tal manera que para cada natural $n \in \mathbb{N}$ tomando el correspondiente número racional $a_n \in \mathbb{Q}$ se obtiene el punto (n, a_n) de la gráfica en la siguiente página.



Límites de sucesiones. Si $\{a_n\}$ es una sucesión de racionales y $L \in \mathbb{Q}$, diremos que $\{a_n\}$ *converge* a L o que L es *límite* de $\{a_n\}$ si para todo racional $\varepsilon > 0$ existe un natural $N = N(\varepsilon)$ (que depende de ε) tal que $|a_n - L| < \varepsilon$ para toda $n \geq N$.

Ésta es una formalización de cuando en lenguaje intuitivo decimos que los valores a_n se "acercan" a L cuando n "crece". Usaremos la notación $L = \lim\limits_{n\to\infty} \{a_n\}$ para indicar que L es límite de $\{a_n\}$.

Ejemplo 5. Si $\{a_n\} = \{a\}$ es la sucesión constante de valor a en $\mathbb{Q}$, entonces $\lim\limits_{n\to\infty} \{a\} = a$.

En efecto, dado $\varepsilon > 0$ en $\mathbb{Q}$, escogemos $N = 1$ y claramente $|a_n - L| = |a - a| = 0 < \varepsilon \ \forall n \geq 1 = N$.

Ejemplo 6. Para la sucesión $\{1/n\}$ se tiene que $\lim\limits_{n\to\infty} \left\{\dfrac{1}{n}\right\} = 0$.

En efecto, dado $\varepsilon > 0$ en $\mathbb{Q}$, queremos hallar $N = N(\varepsilon) \in \mathbb{N}$ tal que $\left|\dfrac{1}{n} - 0\right| = \left|\dfrac{1}{n}\right| = \dfrac{1}{n} < \varepsilon$ si $n \geq N$. Ahora, como queremos que $\frac{1}{n} < \varepsilon$ entonces se debe tener que $n > \frac{1}{\varepsilon}$, y por lo tanto si tomamos $N = [1/\varepsilon] + 1$ (la parte entera de $1/\varepsilon + 1$) se obtiene el resultado deseado.

Ejemplo 7. La sucesión $\{1/2^n\}$ converge a 0.

En efecto, por el ejemplo 2 del capítulo II se tiene que $2^n > n$ para todo $n \in \mathbb{N}$. Se sigue que $0 < (1/2^n) < (1/n)$ y como $\lim\{1/n\} = 0$ por el ejemplo anterior, entonces para todo $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que si $n \geq N$

$$\left|\frac{1}{2^n} - 0\right| < \left|\frac{1}{n} - 0\right| < \varepsilon,$$

i.e., $\lim\{1/2^n\} = 0$.

Ejemplo 8. La sucesión $\{n\}$ no converge ya que dado cualquier racional L siempre existe un natural $n > L$ (propiedad arquimediana de $\mathbb{Q}$).

Cuando una sucesión $\{a_n\}$ de racionales converge a un límite $L \in \mathbb{Q}$, este límite es único:

LEMA V.1. *Sea $\{a_n\}$ una sucesión de racionales y supongamos que L_1 y L_2 son dos límites en $\mathbb{Q}$ de la sucesión. Entonces, $L_1 = L_2$.*

Demostración. Como $L_1 = \lim\{a_n\}$, entonces para toda $\varepsilon > 0$ en $\mathbb{Q}$ existe un $N_1 = N_1(\varepsilon) \in \mathbb{N}$ tal que $|a_n - L_1| < \varepsilon$ para toda $n \geq N_1$. Similarmente, como $L_2 = \lim\{a_n\}$, entonces para toda $\varepsilon > 0$ en $\mathbb{Q}$ existe un $N_2 = N_2(\varepsilon) \in \mathbb{N}$ tal que $|a_n - L_2| < \varepsilon$ para toda $n \geq N_2$.

Si sucediera que $L_1 \neq L_2$, entonces $\varepsilon := \frac{1}{2}|L_1 - L_2| > 0$ en $\mathbb{Q}$ y para este $\varepsilon > 0$ escojamos N_1 y N_2 como antes. Tomando $N = \text{máx}\{N_1, N_2\}$ se sigue que si $n \geq N$ entonces:

$$\begin{aligned} |L_2 - L_1| &= |a_n - L_1 + L_2 - a_n| \leq |a_n - L_1| + |L_2 - a_n| \\ &< \varepsilon + \varepsilon = 2\varepsilon = 2\left(\frac{1}{2}|L_1 - L_2|\right) \\ &= |L_1 - L_2|, \end{aligned}$$

i.e., $|L_1 - L_2| < |L_1 - L_2|$, una contradicción. □

Dada una sucesión $\{a_n\}$ en $\mathbb{Q}$, decimos que la sucesión $\{b_n\}$ es una *subsucesión* de $\{a_n\}$ si existe una *función creciente* $\psi : \mathbb{N} \to \mathbb{N}$ (*i.e.*, $\psi(m) > \psi(n)$ siempre que $m > n$) tal que $\forall k \in \mathbb{N}$ se tiene que $b_k = a_{\psi(k)}$.

EJERCICIO 2. Demuestre que toda subsucesión de una sucesión convergente converge al mismo límite que el de la sucesión dada.

Ejemplo 9. La sucesión $\{(-1)^n\}$ no converge.

Esto se sigue del ejercicio anterior y de la observación de que esta sucesión tiene las dos subsucesiones siguientes: la sucesión constante $\{+1\}$ y la sucesión constante $\{-1\}$, que convergen, por el ejemplo 5, a $+1$ y -1 respectivamente.

EJERCICIO 3. Demuestre que la sucesión $\left\{\dfrac{3n}{2n+1}\right\}$ converge a $3/2$.

EJERCICIO 4. Demuestre que la sucesión $\left\{\dfrac{n+4}{3n+1}\right\}$ converge a $1/3$.

Además de la clasificación en convergentes o no convergentes de las sucesiones de números racionales, necesitaremos las siguientes clases de sucesiones:

(1) Una sucesión de racionales $\{a_n\}$ se dice que es *acotada* si existe un racional $c \in \mathbb{Q}$ tal que $|a_n| \leq c$ para todo n.

(2) Una sucesión de racionales $\{a_n\}$ se dice que es *de Cauchy* si para todo racional $\varepsilon > 0$ existe un natural $N = N(\varepsilon) \in \mathbb{N}$ tal que $|a_m - a_n| < \varepsilon$ para todos los $m, n \geq N$.

LEMA V.2. (1) *Toda sucesión convergente es de Cauchy.*

(2) *Toda sucesión de Cauchy es acotada.*

Demostración. (1) Si $\lim\{a_n\} = L \in \mathbb{Q}$, entonces para toda $\varepsilon > 0$ en $\mathbb{Q}$ existe un $N = N(\varepsilon) \in \mathbb{N}$ tal que $|a_n - L| < \varepsilon/2$ para toda $n \geq N$. Entonces, si $m, n \geq N$, se tiene que

$$|a_m - a_n| = |a_m - L + L - a_n| \leq |a_m - L| + |L - a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

y por lo tanto $\{a_n\}$ es de Cauchy.

(2) Si $\{a_n\}$ es de Cauchy, entonces en particular para $\varepsilon = 1$ existe $N = N(1) \in \mathbb{N}$ tal que $|a_m - a_n| < 1$ si $m, n \geq N$. Entonces, para $n = N$ fijo y $m \geq N$ se tiene que:

$$||a_m| - |a_N|| \leq |a_m - a_N| < 1$$

y por lo tanto $|a_m| - |a_N| < 1$, *i.e.*,

$$|a_m| < |a_N| + 1 \quad \text{para toda } m \geq N,$$

es decir, los valores $|a_m|$, para $m \geq N$, están acotados por el racional $|a_N|+1$.

Ahora, para los términos restantes: $a_1, a_2, \ldots, a_{N-1}$, éstos se acotan por sus valores absolutos y así, tomando

$$c := \text{máx}\{|a_N| + 1, |a_1|, \ldots, |a_{N-1}|\} \in \mathbb{Q}$$

se tiene que $|a_n| \leq c$ para todo $n \in \mathbb{N}$. □

EJERCICIO 5. Si $\{a_n\}$ es una sucesión de Cauchy en $\mathbb{Q}$, demuestre que toda subsucesión de $\{a_n\}$ también es de Cauchy.

EJERCICIO 6. Si $\{a_n\}$ es una sucesión de Cauchy en $\mathbb{Q}$ tal que tiene una subsucesión convergente, demuestre que $\{a_n\}$ converge al mismo límite que el de la subsucesión dada.

Que no toda sucesión de Cauchy en $\mathbb{Q}$ es convergente lo muestra el ejercicio siguiente:

EJERCICIO 7. Considere la sucesión $\{a_n\}$ del ejemplo 4, donde los números racionales a_n están definidos recursivamente como sigue: $a_1 = 1$ y $a_{n+1} := \dfrac{a_n^2 + 2}{2a_n}$. Demuestre que $\{a_n\}$ es de Cauchy y sin embargo $\lim\{a_n\} \notin \mathbb{Q}$. *Sugerencia*: vea los primeros términos de la sucesión $\{a_n\}$ que calculó en el ejemplo 4. Conviértalos a decimales y piense un rato.

Las sucesiones de racionales se pueden sumar y multiplicar en forma natural: si $\{a_n\}$ y $\{b_n\}$ son dos sucesiones en $\mathbb{Q}$, se definen:

SUMA. $\{a_n\} + \{b_n\} := \{a_n + b_n\}$.

PRODUCTO. $\{a_n\}\{b_n\} := \{a_n b_n\}$.

LEMA V.3. *Si $\{a_n\}$ y $\{b_n\}$ son dos sucesiones en $\mathbb{Q}$ tales que $\lim\{a_n\} = L_1 \in \mathbb{Q}$ y $\lim\{b_n\} = L_2 \in \mathbb{Q}$, entonces*

(1) *$\{a_n + b_n\}$ converge en $\mathbb{Q}$ y de hecho*

$$\lim\{a_n + b_n\} = L_1 + L_2.$$

(2) *$\{a_n b_n\}$ converge en $\mathbb{Q}$ y de hecho*

$$\lim\{a_n b_n\} = L_1 L_2.$$

Demostración. (1) Para todo $\varepsilon > 0$ existe $N_1 = N_1(\varepsilon) \in \mathbb{N}$ tal que $|a_n - L_1| < \varepsilon/2$ para todo $n \geq N_1$ y también existe $N_2 = N_2(\varepsilon) \in \mathbb{N}$ tal que $|b_n - L_2| < \varepsilon/2$ para todo $n \geq N_2$. Sea $N = \max\{N_1, N_2\}$; entonces para toda $n \geq N$ se tiene que:

$$|a_n + b_n - (L_1 + L_2)| \leq |a_n - L_1| + |b_n - L_2| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

(2) Observemos primero que

$$(*)\ |a_nb_n - L_1L_2| = |(a_n - L_1)b_n + L_1(b_n - L_2)| \leq |a_n - L_1||b_n| + |b_n - L_2||L_1|.$$

Ahora, como $\{b_n\}$ es acotada por (V.2), entonces existe una constante $c \in \mathbb{Q}$ (digamos, > 0) tal que $|b_n| \leq c$ para toda $n \in \mathbb{N}$ y como $\lim\{a_n\} = L_1$ entonces para todo $\varepsilon > 0$ existe $N_1 \in \mathbb{N}$ tal que $|a_n - L_1| < \varepsilon/c$ siempre que $n \geq N_1$. Si $L_1 = 0$, de $(*)$ se sigue que para toda $n \geq N_1$:

$$|a_nb_n - L_1L_2| = |a_n - L_1||b_n| + 0 \leq |a_n - L_1|c < \frac{\varepsilon}{c}c = \varepsilon,$$

i.e., $\lim\{a_nb_n\} = L_1L_2 = 0$.

Ahora, si $L_1 \neq 0$, como $\lim\{b_n\} = L_2$, existe $N_2 \in \mathbb{N}$ tal que $|b_n - L_2| < \varepsilon/|L_1|$ siempre que $n \geq N_2$. Sea $N = \max\{N_1, N_2\}$; entonces, en $(*)$ para todo $n \geq N$ se tiene que

$$\begin{aligned} |a_nb_n - L_1L_2| &\leq |a_n - L_1||b_n| + |b_n - L_2||L_1| \\ &< \frac{\varepsilon}{c}c + \frac{\varepsilon}{|L_1|}|L_1| = \varepsilon, \end{aligned}$$

i.e., $\lim\{a_nb_n\} = L_1L_2$. □

LEMA V.4. *Si $\{a_n\}$ y $\{b_n\}$ son dos sucesiones de Cauchy en $\mathbb{Q}$, entonces $\{a_n + b_n\}$ y $\{a_nb_n\}$ también son de Cauchy.*

Demostración. (1) Como $\{a_n\}$ y $\{b_n\}$ son de Cauchy, entonces para todo $\varepsilon > 0$ existen $N_1 = N_1(\varepsilon) \in \mathbb{N}$ $N_2 = N_2(\varepsilon) \in \mathbb{N}$ tales que $|a_m - a_n| < \varepsilon/2$ para todo $m, n \geq N_1$ y $|b_m - b_n| < \varepsilon/2$ para todo $m, n \geq N_2$. Sea $N = \max\{N_1, N_2\}$; entonces para toda $m, n \geq N$ se tiene que:

$$|(a_m + b_m) - (a_n + b_n)| \leq |a_m - a_n| + |b_m - b_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

(2) Para el producto observemos que

$$a_mb_m - a_nb_n = (a_m - a_n)b_m + a_n(b_m - b_n)$$

y así

$$|a_mb_m - a_nb_n| = |(a_m - a_n)b_m + a_n(b_m - b_n)| \leq |(a_m - a_n)||b_m| + |a_n||(b_m - b_n)|,$$

donde $\{a_n\}$ y $\{b_n\}$ son acotadas por el lema (V.2) y así existen constantes $c_1, c_2 \in \mathbb{Q}$ (a las que escogemos $\neq 0$) tales que $|a_i| \leq c_1$ y $|b_i| \leq c_2$ para toda $i \in \mathbb{N}$.

Ahora, como $\{a_n\}$ y $\{b_n\}$ son de Cauchy, entonces para todo $\varepsilon > 0$ existen $N_1 = N_1(\varepsilon) \in \mathbb{N}$ $N_2 = N_2(\varepsilon) \in \mathbb{N}$ tales que $|a_m - a_n| < \varepsilon/(2c_1)$ para todo $m, n \geq N_1$ y $|b_m - b_n| < \varepsilon/(2c_2)$ para todo $m, n \geq N_2$. Sea $N = \text{máx}\{N_1, N_2\}$; entonces para toda $m, n \geq N$ se tiene que:

$$|a_m b_m - a_n b_n| \leq |(a_m - a_n)||b_m| + |a_n||(b_m - b_n)| < \frac{\varepsilon}{2c_1} c_1 + \frac{\varepsilon}{2c_2} c_2 = \varepsilon. \qquad \square$$

COROLARIO V.5. *Denotemos con $\mathcal{C}$ al conjunto de sucesiones de Cauchy en $\mathbb{Q}$. Entonces, con las operaciones anteriores $\mathcal{C}$ es un anillo conmutativo con uno.*

Demostración. El lema anterior nos dice que $\mathcal{C}$ es cerrado bajo la suma y producto de sucesiones. Las propiedades de anillo se heredan de las de $\mathbb{Q}$ y sólo indicaremos algunos puntos: el 0 de $\mathcal{C}$ es la sucesión constante $\{0\}$. El inverso aditivo de $\{a_n\} \in \mathcal{C}$ es la sucesión $\{-a_n\}$ que es de Cauchy ya que es el producto de la sucesión constante $\{-1\}$ por $\{a_n\}$. El 1 de $\mathcal{C}$ es la sucesión constante $\{1\}$. $\square$

COROLARIO V.6. *Denotemos con $\mathcal{N}$ al conjunto de sucesiones en $\mathbb{Q}$ que convergen al $0 \in \mathbb{Q}$. Entonces, $\mathcal{N}$ es cerrado bajo sumas y productos. $\mathcal{N} \subsetneq \mathcal{C}$. Más aún, si $\{a_n\} \in \mathcal{C}$ y $\{x_n\} \in \mathcal{N}$, entonces $\{a_n\}\{x_n\} \in \mathcal{N}$.*

Demostración. Que $\mathcal{N}$ es cerrado bajo sumas y productos se sigue del lema (V.4). Como toda sucesión convergente es de Cauchy (V.2), entonces $\mathcal{N} \subseteq \mathcal{C}$ y se tiene que $\mathcal{N} \neq \mathcal{C}$ ya que, por ejemplo $1 = \{1\} \in \mathcal{C} - \mathcal{N}$. La última afirmación la dejamos como un ejercicio. $\square$

EJERCICIO 8. La función natural $\mathbb{Q} \to \mathcal{C}$ que manda cada racional $a \in \mathbb{Q}$ en la sucesión constante $\{a\} \in \mathcal{C}$ respeta las operaciones de ambos anillos y es inyectiva.

EJERCICIO 9. Demuestre que si $\{a_n\} \in \mathcal{C}$ y $\{x_n\} \in \mathcal{N}$, entonces $\{a_n\}\{x_n\} \in \mathcal{N}$.

V.2 El campo de números reales

Usando el subconjunto $\mathcal{N} \subsetneq \mathcal{C}$ definimos una relación de equivalencia en el anillo de sucesiones de Cauchy $\mathcal{C}$ como sigue: si $\{a_n\}, \{b_n\} \in \mathcal{C}$, diremos que $\{a_n\} \sim \{b_n\}$ si su diferencia $\{a_n\} - \{b_n\} \in \mathcal{N}$.

LEMA V.7. $\sim$ *es una relación de equivalencia en* $\mathcal{C}$.

Demostración. Es reflexiva ya que $\{a_n\} - \{a_n\} = \{0\} \in \mathcal{N}$.

Es simétrica ya que si $\{a_n\} - \{b_n\} \in \mathcal{N}$, entonces por (V.6) $\{b_n\} - \{a_n\} = \{-1\}(\{a_n\} - \{b_n\}) \in \mathcal{N}$ ya que $\{-1\} \in \mathcal{C}$.

Es transitiva ya que si $\{a_n\} - \{b_n\} \in \mathcal{N}$ y $\{b_n\} - \{c_n\} \in \mathcal{N}$, entonces

$$\{a_n\} - \{c_n\} = (\{a_n\} - \{b_n\}) + (\{b_n\} - \{c_n\}) \in \mathcal{N}$$

ya que $\mathcal{N}$ es cerrado bajo sumas. □

EJERCICIO 10. Sea $\{a_n\}$ una sucesión de Cauchy en $\mathbb{Q}$. Demuestre que si $\{a'_n\}$ es una subsucesión de $\{a_n\}$ entonces $\{a_n\} \sim \{a'_n\}$.

El conjunto cociente $\mathcal{C}/\sim$ se denota $\mathbb{R}$ y sus elementos, que son clases de equivalencia de sucesiones de Cauchy $\{a_n\}$ en $\mathbb{Q}$, se llaman *números reales* y los denotaremos mediante $[a_n]$.

Operaciones en $\mathbb{R}$. Se tienen operaciones de suma y producto de reales definidos como sigue: sean $\alpha, \beta \in \mathbb{R}$ y escojamos representantes $\{a_n\} \in \alpha$ y $\{b_n\} \in \beta$:

SUMA. Una vez elegidos los representantes anteriores se suman las sucesiones en $\mathcal{C}$, $\{a_n + b_n\} \in \mathcal{C}$ y luego se toma la clase de equivalencia $\alpha + \beta := [a_n + b_n] \in \mathbb{R}$. Por supuesto que hay que probar que esta "definición" no depende de la elección de los representantes en cada clase. Esto se hará en la primera parte del siguiente ejercicio.

PRODUCTO. Los representantes anteriores se multiplican en $\mathcal{C}$, $\{a_n b_n\} \in \mathcal{C}$ y después se toma la clase de equivalencia $\alpha \cdot \beta := [a_n b_n] \in \mathbb{Z}$. Que ésta es una buena definición es el contenido de la segunda parte del ejercicio siguiente:

EJERCICIO 11. Si $\{a_n\} \sim \{a'_n\}$ y $\{b_n\} \sim \{b'_n\}$, demuestre que:

(1) $\{a_n + b_n\} \sim \{a'_n + b'_n\}$.

(2) $\{a_n b_n\} \sim \{a'_n b'_n\}$.

TEOREMA V.8. *Con las operaciones anteriores* $(\mathbb{R}, +, \cdot)$ *es un campo.*

Demostración. Ya hemos visto que $\mathbb{R}$ es cerrado con respecto a las operaciones anteriores. Que la suma es asociativa y conmutativa lo dejamos como un ejercicio. El neutro aditivo de $\mathbb{R}$ es la clase de la sucesión constante $\{0\}$; denotamos este neutro por 0. El inverso aditivo de $\alpha = [a_n] \in \mathbb{R}$ es $[-a_n]$ ya que

$$[a_n] + [-a_n] = [a_n - a_n] = [0] = 0.$$

Denotaremos al inverso aditivo de $[a_n]$ como $-[a_n]$.

Que el producto es asociativo, conmutativo y distribuye a la suma lo dejamos como ejercicio. El neutro multiplicativo de $\mathbb{R}$ es la clase de la sucesión constante $[1]$; denotaremos al neutro multiplicativo por 1.

Si $\alpha = [a_n] \neq 0$ en $\mathbb{R}$, entonces para cualquier representante $\{a_n\} \in [a_n]$ se tiene que $\{a_n\} \notin \mathcal{N}$. Se sigue que $\lim\{a_n\} \neq 0$ y por lo tanto existe un natural $N \in \mathbb{N}$ tal que $a_n \neq 0$ para todo $n \geq N$. Pongamos

$$b_n := \begin{cases} 1 & \text{si } n < N \\ a_n & \text{si } n \geq N. \end{cases}$$

Se tiene entonces que $b_n \neq 0$ para toda n, claramente $\{b_n\}$ es de Cauchy y además $\{b_n\} \sim \{a_n\}$ ya que

$$\{a_n - b_n\} = \{a_1 - 1, a_2 - 1, \ldots, a_{n-1} - 1, 0, \ldots\} \in \mathcal{N}.$$

Hemos así mostrado que todo real $[a_n] \neq 0$ tiene un representante $\{b_n\}$ tal que $b_n \neq 0$ para todo n. Escogiendo este representante $\{b_n\} \in [a_n] \neq 0$, se prueba fácilmente que $\{b_n^{-1}\}$ es de Cauchy y se define $\beta := [b_n^{-1}]$. Se sigue que $\alpha\beta = [a_n][b_n] = [1] = 1$. Denotaremos al inverso multiplicativo de $[a_n]$ como $[a_n]^{-1}$. □

Ejercicio 12. Demuestre la asociatividad y conmutatividad de la suma en $\mathbb{R}$.

Ejercicio 13. Demuestre la asociatividad y conmutatividad del producto en $\mathbb{R}$.

Ejercicio 14. Demuestre que el producto distribuye a la suma en $\mathbb{R}$.

Ejercicio 15. En la demostración del teorema anterior, muestre que la sucesión $\{b_n^{-1}\}$ es de Cauchy. Recuerde que $\{b_n\}$ es de Cauchy y además $\{b_n\} \notin \mathcal{N}$.

Observación. Como todos los elementos $\neq 0$ de $\mathbb{R}$ tienen inverso multiplicativo, se puede definir la división en $\mathbb{R}$ como sigue: sean $\alpha, \beta \in \mathbb{R}$ con $\beta \neq 0$ (por lo que $\beta^{-1} \in \mathbb{R}$). Se define

$$\frac{\alpha}{\beta} := \alpha \cdot \beta^{-1} \in \mathbb{R}.$$

Así como el anillo de enteros $\mathbb{Z}$ se incluye en el campo $\mathbb{Q}$, veremos que $\mathbb{Q}$ se incluye en el campo $\mathbb{R}$:

EJERCICIO 16. Demuestre que la función $\phi : \mathbb{Q} \to \mathbb{R}$ que manda $a \in \mathbb{Q}$ en la clase de la sucesión constante $[a]$ es inyectiva y preserva las operaciones de $\mathbb{Q}$ y $\mathbb{R}$ (es decir, $\phi(a+b) = \phi(a) + \phi(b)$ y $\phi(ab) = \phi(a)\phi(b)$). Nótese que en estas igualdades la suma y producto en los lados izquierdos son los de $\mathbb{Q}$ y los del lado derecho son los de $\mathbb{R}$.

EJERCICIO 17. Demuestre que $\phi(0) = 0$ y que $\phi(1) = 1$, donde en los lados izquierdos el 0 y el 1 son los de $\mathbb{Q}$ y en los lados derechos son los de $\mathbb{R}$.

Gracias a este ejercicio no hay confusión al denotar con los mismos símbolos a los ceros y unos de $\mathbb{Q}$ y de $\mathbb{R}$.

EJERCICIO 18. Demuestre que para todo $a \in \mathbb{Q}$ se tiene que $\phi(-a) = -\phi(a)$.

EJERCICIO 19. Demuestre que para todo $a \in \mathbb{Q}$, si $a \neq 0$ se tiene que $\phi(a^{-1}) = (\phi(a))^{-1}$.

V.3 El orden en $\mathbb{R}$

Para introducir un orden en $\mathbb{R}$ necesitamos definir una clase positiva $\mathbb{R}^+$ en $\mathbb{R}$. Esto se hace como sigue:

$$\mathbb{R}^+ := \{[a_n] \in \mathbb{R} : \exists r > 0 \text{ en } \mathbb{Q} \text{ y } \exists N \in \mathbb{N} \text{ tal que } n > N \Rightarrow a_n \geq r \text{ en } \mathbb{Q}\}.$$

Nótese que esta definición sigue el *dictum: una sucesión la determina su cola infinita*. Observemos para comenzar que $\mathbb{R}^+$ es un conjunto bien definido ya que si $\{a'_n\} \sim \{a_n\}$ y existe $N \in \mathbb{N}$ tal que $\forall n > N$ se tiene que $a_n > 0$, entonces existe $r > 0$ en $\mathbb{Q}$ tal que $a_n \geq r$ para todo $n > N$. Ahora, como $\{a_n\} - \{a'_n\} \to 0$, para el racional $(r/2) > 0$ podemos encontrar un $M \in \mathbb{N}$ tal que $M > N$ y tal que si $m > M$ entonces

$$a_m - a'_m \leq |a_m - a'_m| < r/2$$

por lo que $a_m - (r/2) < a'_m$. Y como de $r \leq a_m$ se sigue que $(r/2) \leq a_m - (r/2)$, estas desigualdades implican que:

$$0 < (r/2) \leq a_m - (r/2) < a'_m$$

y por lo tanto para toda $m > M$ se tiene que $a'_m > 0$, *i.e.*, $[a'_m] \in \mathbb{R}^+$.

LEMA V.9. $\mathbb{R}^+$ *es una clase positiva, es decir:*

(1) $\mathbb{R}^+$ *es cerrado bajo sumas y productos.*

(2) (Tricotomía): *Sea* $a \in \mathbb{R}$. *Entonces se cumple una y sólo una de las afirmaciones siguientes:*

(I) $a \in \mathbb{R}^+$.

(II) $-a \in \mathbb{R}^+$.

(III) $a = 0$.

Demostración. La parte (1) la dejamos como un ejercicio. Para (2), supongamos que $\alpha = [a_n] \in \mathbb{R}$ es $\neq 0$. Entonces como mostramos en la demostración de la existencia de inversos multiplicativos en (V.8), la clase $[a_n] \neq 0$ tiene un representante $\{a_n\}$ con todos los $a_n \neq 0$. Más aún, como $\{a_n\} \notin \mathcal{N}$ entonces $\lim\{a_n\} \neq 0$ por lo que existe un $\varepsilon > 0$ tal que para todo $N \in \mathbb{N}$ existe $n \in \mathbb{N}$ tal que $|a_n| > \varepsilon$ para todo $n > N$. Finalmente, como $\{a_n\}$ es de Cauchy, lo anterior implica que para todo $n > N$ se tiene que $a_n > 0$ o $-a_n > 0$ para n suficientemente grande. Se sigue que $\alpha \in \mathbb{R}^+$ o $-\alpha \in \mathbb{R}^+$. □

EJERCICIO 20. Demuestre que $\mathbb{R}^+$ es cerrado bajo sumas y productos.

EJERCICIO 21. Si $a \in \mathbb{Q}$, demuestre que $a \in \mathbb{Q}^+$ si y sólo si $\phi(a) \in \mathbb{R}^+$.

Se define el orden $<$ en $\mathbb{R}$ en la forma usual: si $\alpha, \beta \in \mathbb{R}$, entonces $\alpha < \beta \Leftrightarrow \beta - \alpha \in \mathbb{R}^+$.

EJERCICIO 22. Demuestre que si $a, b \in \mathbb{Q}$, entonces $a < b$ en $\mathbb{Q} \Leftrightarrow \phi(a) < \phi(b)$ en $\mathbb{R}$.

Si $\alpha, \beta \in \mathbb{R}$ se define $\alpha \leq \beta$ si y sólo si $\alpha < \beta$ o $\alpha = \beta$.

EJERCICIO 23. Demuestre que $\leq$ es una relación reflexiva, antisimétrica y transitiva en $\mathbb{R}$. Demuestre que esta relación es compatible con la suma y el producto por factores positivos.

El valor absoluto en $\mathbb{R}$. Si $\alpha \in \mathbb{R}$ se define su valor absoluto:

$$|\alpha| := \begin{cases} \alpha & \text{si } \alpha \geq 0 \\ -\alpha & \text{si } \alpha < 0. \end{cases}$$

EJERCICIO 24. Si $a, b \in \mathbb{Q}$, demuestre que $|a \quad b| = |\phi(a) - \phi(b)|$, donde a la izquierda se tiene el valor absoluto de $\mathbb{Q}$ y a la derecha se tiene el valor absoluto de $\mathbb{R}$.

EJERCICIO 25. Si $\alpha = [a_n] \in \mathbb{R}$ con los $a_n \in \mathbb{Q}$, demuestre que $|[a_n]| = [|a_n|]$.

EJERCICIO 26. Sean $[a_n], [b_n] \in \mathbb{R}$. Demuestre que si para toda n, $a_n \leq b_n$ en $\mathbb{Q}$, entonces $[a_n] \leq [b_n]$ en $\mathbb{R}$.

EJERCICIO 27. Si $\alpha = [a_n]$, $\beta = [b_n]$, $\gamma = [c_n]$ en $\mathbb{R}$, demuestre que $|\alpha - \beta| \leq |\alpha - \gamma| + |\gamma - \beta|$.

V.4 COMPLETEZ DE $\mathbb{R}$

Las nociones de sucesión, límite, sucesión de Cauchy y de sucesión acotada se definen en $\mathbb{R}$ en forma similar a como se definieron en $\mathbb{Q}$ con la salvedad que ahora el $\varepsilon > 0$ se puede tomar en $\mathbb{R}$. Las propiedades usuales, a saber, (V.1), (V.2), (V.3) y (V.4) tienen sus contrapartes en el caso de $\mathbb{R}$.

EJERCICIO 28. Formule los conceptos mencionados arriba y demuestre las propiedades indicadas.

Nuestro objetivo ahora es probar que, a diferencia de $\mathbb{Q}$, en $\mathbb{R}$ todas las sucesiones de Cauchy convergen (a un número real). Un campo en el cual todas las sucesiones de Cauchy son convergentes se dice que es un *campo completo.* Así, lo que probaremos es que *el campo* $\mathbb{R}$ *es completo.* Éste es un resultado del que no podemos subrayar suficientemente su importancia en toda la matemática, baste decir que el cálculo diferencial e integral depende en mucho de la completez de $\mathbb{R}$. Para probar este teorema necesitaremos algunos preliminares, entre ellos el análogo de la propiedad arquimediana de $\mathbb{Q}$ —véase (IV.11)— para $\mathbb{R}$.

LEMA V.10. *Si $\alpha > 0$ en $\mathbb{R}$, entonces existe $a \in \mathbb{Q}$ tal que $0 < a < \alpha$.*

Demostración. Como $\alpha > 0$, entonces existe $\{a_n\} \in \alpha$ tal que $a_n > 0$ para todo $n \in \mathbb{N}$ y además $\{a_n\} \notin \mathcal{N}$. Entonces, existe un $r \in \mathbb{Q}^+$ tal que $a_i = |a_i| \geq r$ para i arbitrariamente grande.

Ahora, como $\{a_n\}$ es de Cauchy en $\mathbb{Q}$, entonces para $\varepsilon = (1/2)r > 0$ en $\mathbb{Q}$ existe $N \in \mathbb{N}$ tal que $|a_m - a_n| < (1/2)r$ para $m, n \geq N$.

Escojamos i arbitrariamente grande tal que $i \geq N$. Entonces

$$r \leq a_i = a_i - a_m + a_m \leq |a_i - a_m| + |a_m| < \frac{1}{2}r + a_m,$$

i.e.,

$$\frac{1}{2}r = r - \frac{1}{2}r < a_m$$

siempre que $m \geq N$. Se sigue que

$$\left[a_k - \frac{1}{2}r\right] = [a_k] - [(1/2)r] = \alpha - \frac{1}{2}r \geq 0.$$

Finalmente, como $\alpha - (1/3)r > \alpha - (1/2)r \geq 0$, entonces $\alpha > (1/3)r$, por lo que $a := (1/3)r \in \mathbb{Q}$ satisface lo requerido en el lema. □

TEOREMA V.11 (Propiedad arquimediana de $\mathbb{R}$). *Si $\alpha, \beta \in \mathbb{R}$ son tales que $0 < \alpha < \beta$, entonces existe $m \in \mathbb{N}$ tal que $m\alpha > \beta$.*

Demostración. Como $\alpha > 0$, por el lema anterior existe $a \in \mathbb{Q}$ tal que $0 < a < \alpha$. Por otra parte, si $\beta = [b_n]$ con $\{b_n\}$ una sucesión de Cauchy en $\mathbb{Q}$, entonces $\{b_n\}$ es acotada y así existe $b \in \mathbb{Q}$ tal que $|b_n| \leq b$ para todo $n \in \mathbb{N}$ y como $\beta > 0$ en $\mathbb{R}$, entonces podemos suponer que $b_n > 0$ para todo n y consecuentemente $0 < b_n \leq b$ para todo n. Se tiene entonces que $\beta < b$ y por lo tanto $0 < a < \alpha < \beta < b$, *i.e.*, $0 < a < b$ en $\mathbb{Q}$ y así, por la propiedad arquimediana de $\mathbb{Q}$, (IV.11), existe $m \in \mathbb{N}$ tal que $ma > b$. Multiplicando las desigualdades $0 < a < \alpha < \beta < b$ por $m \in \mathbb{N}$ se obtiene que $m\alpha > ma > b > \beta$, *i.e.*, $m\alpha > \beta$ que es lo que se quería. □

Un subconjunto $A \subseteq \mathbb{R}$ se dice que es *denso* si para cada $\alpha \in \mathbb{R}$ existe una sucesión $\{a_n\}$ con $a_n \in A$ para toda n, tal que $\lim\{a_n\} = \alpha$. El lema siguiente nos dice que $\mathbb{Q}$ es denso en $\mathbb{R}$ y que todo número real es límite de una sucesión de Cauchy de números racionales.

LEMA V.12. *Si* $\alpha = [a_n] \in \mathbb{R}$, *entonces* $\lim_{n\to\infty}\{a_n\} = \alpha$. (El límite es en $\mathbb{R}$ identificando los racionales a_n con su imagen en $\mathbb{R}$). *En particular,* $\phi(\mathbb{Q})$ *es denso en* $\mathbb{R}$.

Demostración. Dado $\varepsilon > 0$ en $\mathbb{R}$, por el lema anterior existe $e > 0$ en $\mathbb{Q}$ tal que $0 < e < \varepsilon$. Ahora, como $\{a_n\}$ es de Cauchy en $\mathbb{Q}$, para este $e > 0$ existe un $N = N(e) \in \mathbb{N}$ tal que $|a_m - a_n| < e$ siempre que $m, n \geq N$.

Para un $m \geq N$ dado, si $k \geq N$ se tiene que $|a_m - a_k| < e$, es decir:

$$a_m - a_k < e$$

o

$$a_k - a_m < e.$$

Se sigue que, para $\alpha = [a_n]$:

$$a_m - \alpha \leq e < \varepsilon$$

o

$$\alpha - a_m \leq e < \varepsilon,$$

i.e., $|\alpha - a_m| < \varepsilon$ siempre que $m \geq N$, *i.e.,* $\lim_{m\to\infty}\{a_m\} = \alpha$ en $\mathbb{R}$. □

TEOREMA V.13. $\mathbb{R}$ *es completo, es decir, toda sucesión de Cauchy en* $\mathbb{R}$ *converge en* $\mathbb{R}$.

Demostración. Sea $\{\alpha_n\}$ una sucesión de Cauchy en $\mathbb{R}$. Entonces, para todo $\varepsilon > 0$ en $\mathbb{R}$, existe un $N = N(\varepsilon/3) \in \mathbb{N}$ tal que $|\alpha_m - \alpha_n| < \varepsilon/3$ siempre que $m, n \geq N$.

Ahora, como $\mathbb{Q}$ es denso en $\mathbb{R}$, para cada $\alpha_n \in \mathbb{R}$ si escribimos $\alpha_n = [a_{p,n}]_{p\in\mathbb{N}}$ con $a_{p,n} \in \mathbb{Q}$, por el lema anterior se tiene que $\lim_{p\to\infty}\{a_{p,n}\} = \alpha_n$ y así, para el $\varepsilon > 0$ dado podemos escoger un racional $a_n := a_{p,n}$ tal que $|a_n - \alpha_n| < \varepsilon/3$ si p es suficientemente grande. Mostraremos que la sucesión de racionales $\{a_n\}$ así construida es de Cauchy. En efecto, sea $e > 0$ en $\mathbb{Q}$ y sea $N = N(e) \in \mathbb{N}$ tal que $|\alpha_m - \alpha_n| < e/3$ y también $|a_n - \alpha_n| < e/3$ si $m, n \geq N$. Entonces, para $m, n \geq N$ se tiene que:

$$\begin{aligned} |a_m - a_n| &= |a_m - \alpha_m + \alpha_m - \alpha_n + \alpha_n - a_n| \\ &\leq |a_m - \alpha_m| + |\alpha_m - \alpha_n| + |\alpha_n - a_n| \\ &< \frac{e}{3} + \frac{e}{3} + \frac{e}{3} = e \end{aligned}$$

por lo que $\{a_m\}$ es de Cauchy en $\mathbb{Q}$. Pongamos $\alpha = [a_n] \in \mathbb{R}$. Mostraremos que $\lim\{\alpha_n\} = \alpha$. En efecto, para toda $\varepsilon > 0$ en $\mathbb{R}$ sea $N = N(\varepsilon) \in \mathbb{N}$ tal que $|a_n - \alpha_n| < \varepsilon/2$ si $n \geq N$ como arriba. Ahora, como $\alpha = \lim\{a_n\}$ por el lema previo, entonces para el $\varepsilon > 0$ anterior existe $N' = N'(\varepsilon) \in \mathbb{N}$ tal que $|a_n - \alpha| < \varepsilon/2$ si $n \geq N'$. Sea $M = \max\{N, N'\}$; entonces para $n \geq M$ se tiene que:

$$\begin{aligned} |\alpha_n - \alpha| &= |\alpha_n - a_n + a_n - \alpha| \\ &\leq |\alpha_n - a_n| + |a_n - \alpha| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon, \end{aligned}$$

i.e., $\lim\{\alpha_n\} = \alpha$. □

Supremos e ínfimos. Un subconjunto $A \subseteq \mathbb{R}$ se dice que está *acotado por arriba* si existe un $c \in \mathbb{R}$ tal que $x \leq c$ para todo $x \in A$. Al número c se le llama una *cota superior* de A. Similarmente, un conjunto $A \subseteq \mathbb{R}$ se dice que está *acotado por abajo* si existe un $b \in \mathbb{R}$ tal que $b \leq x$ para todo $x \in A$. Al número b se le llama una *cota inferior* de A.

Ejemplo 10. El conjunto $\{1/n \ : \ n \in \mathbb{N}\} \subseteq \mathbb{R}$ está acotado superiormente por cualquier real $r \geq 1$ y está acotado inferiormente por cualquier real $s \leq 0$.

Ejemplo 11. El conjunto $A = \mathbb{R}^+$ está acotado inferiormente por cualquier real $r \leq 0$, pero no está acotado superiormente.

Si un conjunto $A \subseteq \mathbb{R}$ está acotado superiormente, de todas sus cotas superiores podemos considerar la menor de ellas. A continuación probaremos que esta cota superior menor existe. Similarmente, si A está acotado inferiormente podemos considerar la mayor de todas las cotas inferiores y probaremos que este número existe:

TEOREMA V.14. *Sea $A \subseteq \mathbb{R}$ un conjunto no vacío.*

(1) *Si A está acotado superiormente, entonces existe un único número real s tal que:*

(I) *s es cota superior de A.*

(II) *s es la menor cota superior de A, i.e., para toda $\varepsilon > 0$ en $\mathbb{R}$ existe $x \in A$ tal que $s - \varepsilon < x$.*

(2) *Análogamente, si A está acotado inferiormente, entonces existe un único número real t tal que:*

(I) *t es cota inferior de A.*

(II) *t es la mayor cota inferior de A, i.e., para toda $\varepsilon > 0$ en $\mathbb{R}$ existe $x \in A$ tal que $x < t + \varepsilon$.*

La menor cota superior s de A se llama el *supremo* de A y se denota por $s = \sup(A)$.
La mayor cota inferior t de A se llama el *ínfimo* de A y se denota por $t = \text{ínf}(A)$.

Demostración. (1) Sea $b \in \mathbb{R}$ cualquier cota superior de A y sea $x \in A$ y sea $x \in A$. Como $\mathbb{R}$ es arquimediano, para los reales $b, -x$, existen enteros positivos $M, -m \in \mathbb{N}$ tales que $M > b$ y $-m > -x$. Se sigue que $m < x \leq b < M$.

Ahora, para cada natural $k \in \mathbb{N}$ pongamos

$$S_k := \{j \in \mathbb{Z} \ : \ \frac{j}{2^k} \quad \text{es una cota superior de } A\}.$$

Observe que si $j \leq 2^k m$, entonces $(j/2^k) \leq m < x$ con $x \in A$, por lo que $j \notin S_k$. Se sigue que S_k está acotado por abajo. Por otra parte, como $2^k M \in S_k$, entonces $S_k \neq \emptyset$. Por el principio del buen orden se sigue que S_k tiene un elemento menor, digamos j_k. Definamos $a_k := j_k/2^k$, para $k = 1, 2, 3, \ldots$. Por definición de j_k se tiene que

$$(*) \quad \frac{2j_k}{2^{k+1}} = \frac{j_k}{2^k} = a_k \quad \text{es una cota superior de } A \quad \text{y} \quad \frac{2j_k - 2}{2^{k+1}} \quad \text{no lo es.}$$

Se sigue que

$$j_{k+1} = 2j_k \quad \text{o} \quad j_{k+1} = 2j_k - 1$$

por lo que

$$a_{k+1} = \frac{2j_k}{2^{k+1}} = a_k \quad \text{o} \quad a_{k+1} = \frac{2j_k - 1}{2^{k+1}} = a_k - \frac{1}{2^{k+1}}$$

y por lo tanto

$$a_{k+1} \leq a_k \quad \text{y} a_k - a_{k+1} \leq \frac{1}{2^{k+1}} \quad \text{para } k = 1, 2, 3, \ldots .$$

Ahora, si $\ell > k \geq 1$, entonces

$$\begin{aligned} 0 \leq a_k - a_\ell &= (a_k - a_{k+1}) + (a_{k+1} - a_{k+2}) + \cdots + (a_{\ell-1} - a_\ell) \\ &\leq \frac{1}{2^{k+1}} + \frac{1}{2^{k+2}} + \cdots + \frac{1}{2^\ell} \\ &= \frac{1}{2^{k+1}}\left(1 + \frac{1}{2} + \cdots + \frac{1}{2^{\ell-k-1}}\right) \\ &= \frac{1}{2^{k+1}}\left(2 - \frac{1}{2^{\ell-k-1}}\right) < \frac{1}{2^k}. \end{aligned}$$

Se tiene entonces que

$$|a_k - a_\ell| = a_k - a_\ell < 1/2^k$$

siempre que $\ell \geq k \geq 1$. Ahora, por el ejemplo 7, la sucesión $\{1/2^k\}$ converge a cero y por lo tanto la desigualdad anterior implica que $\{a_k\}$ es una sucesión de Cauchy y como $\mathbb{R}$ es completo, entonces $\lim\{a_k\} =: a \in \mathbb{R}$. Es claro que $a_k \geq a$. Probaremos que $a = \sup(A)$:

(I) Mostraremos primero que a es cota superior de A. En efecto, si esto no fuera el caso, entonces existiría un $x \in A$ tal que $x > a$ y por lo tanto existiría un natural $k \in \mathbb{N}$ tal que $a_k - a = |a_k - a| < x - a$, *i.e.*, $a_k < x$, lo cual contradice el hecho $(*)$ de que a_k es cota superior de A. Se sigue que a es cota superior de A.

(II) Mostraremos que a es la menor cota superior de A. En efecto, si existiera otra cota superior a' de A tal que $a' < a$, escojamos un natural k tal que $(1/2^k) < a - a'$. Se tiene entonces que

$$a_k - \frac{1}{2^k} \geq a - \frac{1}{2^k} > a - (a - a') = a'$$

y así $a - \dfrac{1}{2^k}$ sería una cota superior de A, en contradicción con $(*)$ y con el hecho de que $a_k - \dfrac{1}{2^k} = \dfrac{j_k - 1}{2^k}$ por definición de a_k. Se sigue que $a = \sup(A)$. □

EJERCICIO 29. Demuestre la parte (2) del teorema anterior.

Ejemplo 12. Para el conjunto $A = \{1/n\}$ del ejemplo 10, se tiene que $\sup(A) = 1$ e $\text{ínf}(A) = 0$.

EJERCICIO 30. Si $A \subseteq \mathbb{R}$ es un conjunto no vacío acotado por abajo, demuestre que el conjunto $-A := \{-x \ : \ x \in A\}$ es acotado por arriba. Demuestre que

$$\text{ínf}(A) = -\sup(-A).$$

EJERCICIO 31. Si $\emptyset \neq A \subseteq B \subseteq \mathbb{R}$ y B es acotado por arriba y por abajo, demuestre que $\text{ínf}(B) \leq \text{ínf}(A) \leq \sup(A) \leq \sup(B)$.

Arriba hemos mostrado cómo construir un campo ordenado completo que contiene a $\mathbb{Q}$ y es arquimediano. Podríamos preguntarnos si existen otros campos ordenados completos arquimedianos (*i.e.*, que satisfacen la propiedad arquimediana) que contienen a $\mathbb{Q}$; sin embargo, la respuesta es que esto no es posible:

TEOREMA V.15. *Supongamos que $\mathbb{R}_1$ y $\mathbb{R}_2$ son dos campos ordenados completos y arquimedianos que contienen a $\mathbb{Q}$. Sean $\mathbb{R}_1^+$ y $\mathbb{R}_2^+$ sus clases positivas respectivas. Entonces, existe una función $\psi : \mathbb{R}_1 \to \mathbb{R}_2$ tal que:*

(1) *ψ es biyectiva.*

(2) *ψ preserva las operaciones de $\mathbb{R}_1$ y $\mathbb{R}_2$, i.e., para todo $x, y \in \mathbb{R}_1$ se tiene que*

$$\psi(x + y) = \psi(x) + \psi(y)$$
$$\psi(xy) = \psi(x)\psi(y).$$

(3) *$x \in \mathbb{R}_1^+$ si y sólo si $\psi(x) \in \mathbb{R}_2^+$.*

Demostración. Sean $0, 1 \in \mathbb{R}_1$ y $0', 1' \in \mathbb{R}_2$ los neutros aditivos y multiplicativos correspondientes. Definiremos primero a ψ en la copia de $\mathbb{Q}$ metida en $\mathbb{R}_1$, comenzando con los neutros anteriores:

$$\psi(0) = 0'$$
$$\psi(1) = 1'$$

y para $m \in \mathbb{Z}$ se define $\psi(m \cdot 1) = m \cdot 1'$. Si $n \in \mathbb{Z} - \{0\}$ se definen

$$\psi\left(\frac{1}{n} \cdot 1\right) = \frac{1}{n} \cdot 1'$$
$$\psi\left(\frac{m}{n} \cdot 1\right) = \frac{m}{n} \cdot 1'.$$

Esto define ψ en $\mathbb{Q} = \mathbb{Q} \cdot 1 \subseteq \mathbb{R}_1$. Finalmente, si $x \in \mathbb{R}_1 - \mathbb{Q} \cdot 1$ se define

$$\psi(x) := \sup \left\{ \frac{m}{n} \cdot 1' : \frac{m}{n} \cdot 1 < x \right\}.$$

Se deja como un ejercicio el probar que ψ tiene las propiedades requeridas. □

EJERCICIO 32. Termine la demostración anterior.

EJERCICIO 33. Si $\{a_n\}$ es una sucesión decreciente en $\mathbb{R}$, *i.e.*, $a_1 \geq a_2 \geq a_3 \geq \ldots$, y si $a = \text{ínf}\{a_n\}$, demuestre que $\text{lím}\{a_n\} = a$. El recíproco también es cierto.

EJERCICIO 34. Usando el ejercicio anterior, demuestre que la existencia de supremos en $\mathbb{R}$ implica que $\mathbb{R}$ es completo.

En la demostración de la existencia de supremos en $\mathbb{R}$ se usó que $\mathbb{R}$ es completo. Así, este ejercicio nos dice que la completez de $\mathbb{R}$ es equivalente a la existencia de supremos para subconjuntos acotados no vacíos de $\mathbb{R}$.

Observación. Existen varias construcciones de los números reales además de la que nosotros vimos, en particular una construcción importante se debe a R. Dedekind, mediante el empleo de *cortaduras* (véase, por ejemplo, W. Rudin, *Principles of Mathematical Analysis,* McGraw-Hill), o mediante expansiones decimales (véase, por ejemplo, H. Cárdenas, E. Lluis, F. Raggi, F. Tomás, *Álgebra superior,* Trillas), y el teorema anterior nos dice que todas estas construcciones nos dan esencialmente el mismo campo, al que llamaremos el *campo de los números reales.*

V.5 PROYECTO 3: LOS NÚMEROS p-ÁDICOS

En este proyecto, se busca mostrar cómo el valor absoluto de $\mathbb{Q}$ puede ser "desprivilegiado", exhibiendo una familia de "valores absolutos" en $\mathbb{Q}$ que tienen propiedades suficientemente similares a las del valor absoluto (que ahora llamaremos *usual*) de $\mathbb{Q}$ que estudiamos en el capítulo anterior, de tal forma que tienen el derecho a ser llamados *valores absolutos.* Una vez hecho lo anterior, se definen las nociones de *sucesión*, *límite*, *sucesión de Cauchy*, etc., y se esboza cómo construir ciertos campos, que contienen a $\mathbb{Q}$, son

completos y tales que $\mathbb{Q}$ es denso en ellos. Es decir, estos nuevos campos son análogos a $\mathbb{R}$. Originalmente estos campos se estudiaron por sus aplicaciones aritméticas; sin embargo, recientemente han encontrado diversas aplicaciones, incluyendo a la física.

La idea de la construcción de estos nuevos valores absolutos en $\mathbb{Q}$ es la siguiente: dado un número primo $p \in \mathbb{Z} \subseteq \mathbb{Q}$, queremos decir cuándo dos números racionales están *cerca*, en un sentido que involucre al primo p; en particular, queremos ver cuándo un número racional $x \in \mathbb{Q}$ está *cerca* del $0 \in \mathbb{Q}$, *i.e.*, que su *valor absoluto* sea pequeño. Para proceder formalmente, al primo p le queremos asociar una función $|\ |_p$ que asigna a cada racional $x \in \mathbb{Q}$ su *valor absoluto* $|x|_p \in \mathbb{Q}$. Para comenzar, al racional $0 \in \mathbb{Q}$ le asociamos el valor absoluto $|0|_p = 0$; luego, notamos que cada número racional $x = a/b$ diferente de cero se puede escribir de forma única como

$$x = \frac{a}{b} = p^r \frac{a'}{b'}$$

con $r, a', b' \in \mathbb{Z}$ y $p \nmid a'b'$. Se define entonces $|x|_p := p^{-r}$. La función $|\ |_p$ satisface las propiedades siguientes:

PROPOSICIÓN V.16. *Para cualesquiera $x, y \in \mathbb{Q}$,*

(I) $|x|_p \geq 0$ *y* $|x|_p = 0$ *si y sólo si* $x = 0$.

(II) $|xy|_p = |x|_p |y|_p$.

(III) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

Demostración. Las partes (1) y (2) son fáciles. La parte (3) es obvia si uno de los sumandos es el 0. Supongamos entonces que $x \neq 0$, $y \neq 0$ y escribamos

$$x = p^r \frac{a}{b} \quad \text{y} \quad y = p^s \frac{c}{d},$$

con $a, b, c, d, r, s \in \mathbb{Z}$ tales que $p \nmid ab$ y $p \nmid cd$, de tal forma que $|x|_p = p^{-r}$ y $|y|_p = p^{-s}$; supongamos además que $r \geq s$. Entonces,

$$x + y = p^r \frac{a}{b} + p^s \frac{c}{d} = p^s \left(\frac{p^{r-s} ad + bc}{bd} \right) = p^s \frac{u}{v}$$

donde $p \nmid bd$ y $v | bd$, por lo que $p \nmid v$. Se sigue que

$$x + y = p^s \frac{u}{v} = p^{s+t} \frac{w}{v}$$

para algún entero $t \geq 0$, y por lo tanto

$$|x+y|_p = \left|p^{s+t}\frac{w}{v}\right|_p = p^{-s-t} \leq p^{-s} = \max\{p^{-r}, p^{-s}\} = \max\{|x|_p, |y|_p\},$$

como se quería. □

Nótese que la desigualdad (III) implica la desigualdad del triángulo usual:

$$|x+y|_p \leq |x|_p + |y|_p.$$

Así, la función $|\ |_p$ satisface propiedades análogas a las del valor absoluto usual de $\mathbb{Q}$, con la salvedad que satisface una propiedad más fuerte que la desigualdad del triángulo. Diremos que $|\ |_p$ es un *valor absoluto p-ádico en* $\mathbb{Q}$.

EJERCICIO 35. Demuestre que:

(1) $|1|_p = 1$.

(2) $|-a|_p = |a|_p$ para todo $a \in \mathbb{Q}$.

(3) $|a^{-1}|_p = 1/|a|_p$ para todo $a \in \mathbb{Q} - \{0\}$.

El ejercicio siguiente nos muestra la primera diferencia entre el valor absoluto usual y el valor absoluto p-ádico:

EJERCICIO 36. Si $|a|_p \neq |b|_p$, entonces $|a+b|_p = \max\{|a|_p, |b|_p\}$.

Las consecuencias de esta última propiedad son bastante sorprendentes:

EJERCICIO 37. Demuestre que, con la distancia inducida por el valor absoluto p-ádico, todo "triángulo" es isósceles y todo punto interior de una bola abierta es un centro de la bola.

Recordemos que, en $\mathbb{Q}$, el axioma de Arquímedes dice que, dado un racional $a \neq 0$ y cualquier otro racional b, para el valor absoluto usual $|\ |$ de $\mathbb{Q}$ se tiene que $|na| > |b|$ para un número natural n suficientemente grande. Ahora, si en $\mathbb{Q}$ consideramos el nuevo valor absoluto p-ádico, entonces para todo natural n se tiene que $n = 1 + \cdots + 1 \in \mathbb{Q}$ satisface que $|n|_p \leq \max\{|1|_p\} = 1$ y por lo tanto, para todo $a \in \mathbb{Q}$ y todo $n \in \mathbb{N}$:

$$|na|_p = |n|_p|a|_p \leq |a|_p$$

y así no se satisface el axioma de Arquímedes. Decimos entonces que el valor absoluto p-ádico es un *valor absoluto no arquimediano* en $\mathbb{Q}$.

Con el valor absoluto $|\ |_p$ podemos definir, en forma totalmente análoga a la usual, los conceptos de *sucesión de Cauchy*, *límite* de una sucesión, etc., sin embargo, algunas cosas son bastante extrañas en este contexto, como el ejemplo siguiente muestra:

EJERCICIO 38. Considere el primo $p = 7$ y las congruencias

$$x^2 \equiv 2 \text{ mód } 7^n.$$

- Para $n = 1$ observe que la congruencia $x^2 \equiv 2$ mód 7 tiene las soluciones $x \equiv 3$ mód 7 y $x \equiv -3$ mód $7 \equiv 4$ mód 7.
- Para $n = 2$ observe que cualquier solución de la congruencia $x^2 \equiv 2$ mód 7^2 al reducirla módulo 7 debe dar una solución de la congruencia $x^2 \equiv 2$ mód 7. Encuentre las soluciones de la congruencia $x^2 \equiv 2$ mód 7^2.
- Demuestre que para cada $n \geq 1$ la congruencia $x^2 \equiv 2$ mód p^n tiene a lo más dos soluciones.
- Demuestre que dada una solución a_n de la congruencia $x^2 \equiv 2$ mód 7^n, existe una única solución a_{n+1} de la congruencia $x^2 \equiv 2$ mód 7^{n+1} tal que $a_{n+1} \equiv a_n$ mód 7^n.
- Calcule algunos términos de la sucesión $\{a_n\}$ de soluciones de la congruencia $x^2 \equiv 2$ mód 7^n; por ejemplo, muestre que

$$\{a_n\} = (3, 10, 108, 2166, \ldots).$$

- Demuestre que la sucesión $\{a_n\}$ anterior es de Cauchy con el valor absoluto 7-ádico. ¡Ésta sí que es una sucesión de Cauchy que viola todas nuestras intuiciones acerca de lo que significa *estar cerca!*

Recordemos ahora que, si $|\ |$ es el valor absoluto usual de $\mathbb{R}$ y si $\{a_n\}$ es una sucesión de Cauchy de números reales, entonces $\lim_{n\to\infty} |a_{n+1} - a_n| = 0$. Sin embargo, el recíproco es falso. Por ejemplo, si $\{a_n\}$ es una sucesión de reales que converge a 0 y si ponemos $s_n := a_1 + \cdots + a_n$, entonces se tiene

que $\lim_{n\to\infty} |s_{n+1} - s_n| = \lim_{n\to\infty} |a_n| = 0$; sin embargo, puede suceder que la sucesión $\{s_n\}$ no sea de Cauchy, e incluso puede que no sea convergente; el ejemplo típico es el de la sucesión $\{a_n\} = \{1/n\}$. Sin embargo, para el campo $\mathbb{Q}$ con el valor absoluto p-ádico, se tiene que:

LEMA V.17. *Sea $\{a_n\}$ una sucesión en $\mathbb{Q}$ con el valor absoluto p-ádico. Entonces, $\{a_n\}$ es de Cauchy si y sólo si $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$.*

Demostración. Sólo necesitamos probar que si $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$ entonces $\{a_n\}$ es de Cauchy. Para esto, notemos que como este límite es 0, entonces para todo $\varepsilon > 0$ existe un N tal que si $n > N$, entonces $|a_{n+1} - a_n|_p < \varepsilon$.

Escribamos $m = n + r > n$ y observemos que

$$\begin{aligned} |a_m - a_n|_p &= |a_{n+r} - a_{n+r-1} + a_{n+r-1} - a_{n+r-2} + \cdots + a_{n+1} - a_n|_p \\ &\leq \text{máx}\{|a_{n+r} - a_{n+r-1}|_p, |a_{n+r-1} - a_{n+r-2}|_p, \ldots, |a_{n+1} - a_n|_p\} \\ &< \varepsilon. \end{aligned}$$

□

Sin embargo, al campo $\mathbb{Q}$ con el valor absoluto p-ádico le sucede algo similar a lo que le sucede a $\mathbb{Q}$ con el valor absoluto usual: existen sucesiones de Cauchy en $\mathbb{Q}$ que no convergen en $\mathbb{Q}$:

EJERCICIO 39. Consideremos la sucesión $\{a_n\}$ del ejercicio anterior con el valor absoluto 7-ádico de $\mathbb{Q}$. Sea $s_n = a_1 + a_2 + \cdots + a_n$ para cada $n \geq 1$. Entonces tenemos una nueva sucesión en $\mathbb{Q}$, a saber $\{s_n\}$. Por el lema anterior, $\{s_n\}$ es de Cauchy (con el valor absoluto 7-ádico). Demuestre que la sucesión $\{s_n\}$ no converge en $\mathbb{Q}$. De hecho, si denotamos por $\alpha = \lim_{n\to\infty} \{s_n\}$ (dondequiera que este límite viva), demuestre que α es una raíz de la ecuación $x^2 = 2$, *i.e.* $\alpha = \sqrt{2}$. ¡Este ejercicio muestra que la sucesión $\{s_n\}$ converge a $\sqrt{2}$ en el valor absoluto 7-ádico!

En forma totalmente análoga a como, usando el valor absoluto usual en $\mathbb{Q}$, se completó el campo $\mathbb{Q}$ para obtener el campo $\mathbb{R}$ de los números reales, usando ahora el valor absoluto p-ádico $|\ |_p$ se puede completar el campo $\mathbb{Q}$ para obtener un nuevo campo, llamado el *campo de los números p-ádicos*, denotado por $\mathbb{Q}_p$. Así, el ejercicio anterior nos dice que $\sqrt{2} \in \mathbb{Q}_7$. En forma análoga a como el valor absoluto usual de $\mathbb{Q}$ se extendió al valor absoluto usual de $\mathbb{R}$, el valor absoluto p-ádico de $\mathbb{Q}$ se extiende a un valor absoluto de

$\mathbb{Q}_p$ al que seguiremos denotando con $|\ |_p$. Los campos $\mathbb{Q}_p$ pueden parecer extraños comparados con $\mathbb{R}$:

EJERCICIO 40. Procediendo en forma análoga al ejercicio anterior, demuestre que la ecuación $x^2+1=0$ tiene una solución en $\mathbb{Q}_5$, *i.e*, que $\sqrt{-1}\in\mathbb{Q}_5$. Sin embargo, muestre que $x^2+1=0$ no tiene una solución en $\mathbb{Q}_7$, *i.e.*, $\sqrt{-1}\notin\mathbb{Q}_7$.

Uno podría preguntarse ¿cómo se ven los elementos de $\mathbb{Q}_p$?, por ejemplo, ¿cómo se ve el número

$$\alpha=\lim_{n\to\infty}\{s_n\}=\lim_{n\to\infty}\{3+10+108+2166+\cdots+a_n\}$$

del ejercicio (39), en el campo $\mathbb{Q}_7$? Para responder a esto, comenzamos recordando que los sumandos a_n de α se obtuvieron como soluciones de congruencias de la forma

$$x^2\equiv 2\ (\text{mód}\ 7^n).$$

Así, puede parecer natural considerar la *expansión en base* 7 de cada una de estas soluciones:

$$\begin{aligned}3&=3\\10&=3+1\times 7\\108&=3+1\times 7+2\times 7^2\\2166&=3+1\times 7+2\times 7^2+6\times 7^3\\&\vdots\end{aligned}$$

por lo que

$$\begin{aligned}\alpha&=3+10+108+2166+\cdots\\&=3+(3+1\times 7)+(3+1\times 7+2\times 7^2)\\&\quad+(3+1\times 7+2\times 7^2+6\times 7^3)+\cdots\\&=3+1\times 7+2\times 7^2+6\times 7^3+\cdots,\end{aligned}$$

lo cual se parece bastante a la expansión decimal (en base 10) de un número real. Decimos que la anterior es la expansión 7-ádica de α. ¿Puede explicar cómo hicimos la simplificación en el último renglón de la expresión 7-ádica de α? Note que el problema es que al sumar dos racionales (enteros, en el caso considerado) puede suceder que la suma sea mayor que 7, en cuyo caso hacemos lo usual *acarreando lo que se pasa* al siguiente sumando.

Los números p-ádicos desempeñan un papel muy importante en la teoría de números y aparecieron al resolver familias de congruencias módulo la potencia de un primo, como la esbozada en el caso de potencias de 7, de alguna manera simplificando problemas de tipo general al concentrarse en un sólo primo. Existen teoremas muy importantes que explotan las analogías y diferencias entre los campos $\mathbb{Q}_p$ y $\mathbb{R}$. El lector interesado se beneficiaría si hace el esfuerzo de leer algo de la referencia siguiente (tal vez tendría que esperar a madurar sus conocimientos de álgebra y cálculo antes de proseguir) y espero que este proyecto haya alimentado su curiosidad.

V.5.1 Bibliografía

[1] Gouvêa, F., *p-adic numbers*, Springer Verlag, Berlín, 1993.

V.6 Apéndice: El campo $\mathbb{R}$, un enfoque axiomático

En este capítulo V, siguiendo ideas similares a las de los capítulos anteriores, se ha construido el campo de los números reales $\mathbb{R}$, y se ha probado que es un *campo arquimediano completo*. En este apéndice se hace un resumen de las propiedades de $\mathbb{R}$ que se obtuvieron en el capítulo V, poniéndolas en contexto y estudiándolas en general, para al final asumir la existencia del campo $\mathbb{R}$ con estas propiedades. Este enfoque axiomático puede ser una primera aproximación al estudio del campo de números reales, importante para el desarrollo del cálculo diferencial e integral, en el entendido que, posteriormente, al madurar los conocimientos de matemáticas del lector, podrá regresar a estudiar la construcción de $\mathbb{R}$, ya sea por el método que desarrollamos, usando sucesiones de Cauchy o mediante cortaduras de Dedekind.

V.6.1 Propiedades de campo de $\mathbb{R}$

Recordemos que un *campo* K es un anillo conmutativo con uno, en el cual $1 \neq 0$ y todo elemento distinto de 0 tiene un inverso multiplicativo. En forma explícita, un *campo* es un conjunto no vacío K junto con dos operaciones, *suma* y *producto*, *i.e.*, junto con dos funciones

$$+ : K \times K \to K \qquad \text{y} \qquad \cdot : K \times K \to K$$

para las cuales usaremos la notación siguiente: si $(a, b) \in K \times K$ su imagen bajo $+$ se denota $a + b \in K$ y su imagen bajo el producto se denota $a \cdot b \in K$. Recordemos que al decir que la suma y el producto son funciones de $K \times K \to K$ esto quiere decir que a cada par ordenado $(a, b) \in K \times K$ le corresponde, bajo la suma, un único elemento $a + b \in K$ y similarmente para el producto. En ocasiones se dice que la suma y el producto son *operaciones cerradas* en K. Para que K sea un campo se requiere que sus operaciones satisfagan los axiomas siguientes:

I. Propiedades de la suma.

1. La suma es *asociativa*, es decir, para cualesquiera $a, b, c \in K$ se tiene que $a + (b + c) = (a + b) + c$.

2. La suma es *conmutativa*, *i.e.*, para cualesquiera $a, b \in K$ se tiene que $a + b = b + a$.

3. Existe un *neutro aditivo*, *i.e.*, existe un elemento $0 \in K$ tal que para todo $a \in K$ se tiene que $a + 0 = a$.

4. Cada elemento $a \in K$ tiene un *inverso aditivo*, *i.e.*, dado $a \in K$ existe un elemento $a' \in K$ tal que $a + a' = 0$. Al elemento $a' \in K$ se le llama un inverso aditivo del elemento $a \in K$.

II. Propiedades del producto.

1. El producto es *asociativo*, es decir, para cualesquiera $a, b, c \in K$ se tiene que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

2. El producto es *conmutativo*, *i.e.*, para cualesquiera $a, b \in K$ se tiene que $a \cdot b = b \cdot a$.

3. Existe un *neutro multiplicativo*, *i.e.*, existe un elemento $1 \in K$, con $1 \neq 0$, tal que para todo $a \in K$ se tiene que $a \cdot 1 = a$.

4. Cada elemento $a \in K$ distinto de 0 tiene un *inverso multiplicativo*, *i.e.*, dado $a \in K$ con $a \neq 0$, existe un elemento $a'' \in K$ tal que $a \cdot a'' = 1$. Al elemento $a'' \in K$ se le llama un inverso multiplicativo del elemento $a \in K$, $a \neq 0$.

III. Relación entre la suma y el producto.

1. La suma y el producto satisfacen la *propiedad distributiva*, es decir, para cualesquiera $a, b, c \in K$ se tiene que $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Nótese que si quitamos el axioma II.4, un campo K es un anillo conmutativo con uno y, por lo tanto, satisface las propiedades siguientes que se probaron en § III.1:

Lema V.18. *Si $(K, +, \cdot)$ es un campo, entonces:*

1) El neutro aditivo de K es único, es decir, si 0 y $0'$ son dos neutros aditivos de K, entonces $0 = 0'$.

2) El neutro multiplicativo de K es único, es decir, si 1 y $1'$ son dos neutros multiplicativos de K, entonces $1 = 1'$.

3) El inverso aditivo de un elemento $a \in K$ es único, i.e., si $a \in K$ y a' y a'' son dos inversos aditivos de a en K, entonces $a' = a''$.

Al (único) inverso aditivo de $a \in K$ lo denotaremos mediante $-a$. Por definición este elemento satisface que $a + (-a) = 0$.

4) El inverso multiplicativo de un elemento $a \in K$, $a \neq 0$, es único, i.e., si $a \in K - \{0\}$ y a' y a'' son dos inversos multiplicativos de $a \neq 0$ en K, entonces $a' = a''$.

Al (único) inverso multiplicativo de $a \in K$, $a \neq 0$, lo denotaremos mediante a^{-1}. Por definición este elemento satisface que $a \cdot a^{-1} = 1$.

5) Para todo $a \in K$ se tiene que $-(-a) = a$

6) Para todo $a \in K$, $a \neq 0$, se tiene que $\left(a^{-1}\right)^{-1} = a$

7) Para todo $a \in K$ se tiene que $a \cdot 0 = 0$.

8) $a(-b) = -(ab)$.

9) $(-a)b = -(ab)$.

10) $(-a)(-b) = ab$.

11) $(-1)a = -a$. □

EJERCICIO 41. Demuestre el lema anterior sin ver los resultados correspondientes del capítulo III.

EJERCICIO 42. Si K es un campo y $a, b \in K$, demuestre que la ecuación $a + x = b$ tiene una única solución en K.

EJERCICIO 43. Si K es un campo y $a, b \in K$, con $a \neq 0$, demuestre que la ecuación $a \cdot x = b$ tiene una única solución en K.

EJERCICIO 44. Demuestre que todo campo es un dominio entero.

Ejemplo 13. En el capítulo IV estudiamos el *campo de números racionales* $\mathbb{Q}$ y, al inicio del capítulo V, mostramos que si p es un entero primo, entonces $\sqrt{p}$ no es un número racional. En particular, $\sqrt{2} \notin \mathbb{Q}$. Consideremos ahora el conjunto

$$K := \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\},$$

por ejemplo, K contiene a elementos como $2 + 3\sqrt{2}$, $1 - 5\sqrt{2}$, $\frac{3}{4} - \frac{7}{2}\sqrt{2}$, $10 + \frac{1}{25}\sqrt{2}$. Note que K contiene a $\mathbb{Q}$, ya que si $a \in \mathbb{Q}$, entonces $a = a + 0\sqrt{2} \in K$; también se tiene que $\sqrt{2} = 0 + 1\sqrt{2} \in K$, por lo que $\mathbb{Q} \subsetneq K$. En el conjunto K definimos las operaciones suma y producto como sigue: si $\alpha = a + b\sqrt{2}$ y $\beta = c + d\sqrt{2}$ son dos elementos de K, es decir, $a, b, c, d \in \mathbb{Q}$, se definen

SUMA:

$$\alpha + \beta := (a + c) + (b + d)\sqrt{2}$$

y

PRODUCTO:

$$\alpha \cdot \beta := (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

(multiplicando término a término y al final se simplifica recordando que $\sqrt{2}\sqrt{2} = 2$). Claramente la suma y producto son operaciones cerradas en K y se verifica fácilmente que K es un campo que contiene propiamente a $\mathbb{Q}$.

EJERCICIO 45. Verifique que, con las operaciones anteriores, K es un campo.

Ejemplo 14. Considere el conjunto $K = \{0, 1\}$ (del ejercicio 20 del capítulo III) donde los símbolos x los sumamos y multiplicamos de acuerdo con las tablas siguientes:

SUMA:

+	0	1
0	0	1
1	1	0

PRODUCTO:

•	0	1
0	0	0
1	0	1

Es claro que K es un campo.

EJERCICIO 46. Considere el conjunto

$$\mathbb{Q}(i) := \{a + bi \ : \ a, b \in \mathbb{Q}, \ \ i^2 = -1\},$$

donde i es un símbolo que satisface que $i^2 = -1 \in \mathbb{Q}$ y sus potencias se manejan formalmente a partir de lo anterior. Si $\alpha = a + bi$ y $\beta = c + di$ son dos elementos de $\mathbb{Q}(i)$, se definen

$$\alpha + \beta := (a + c) + (b + d)i$$

y

$$\alpha \cdot \beta := (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Demuestre que $\mathbb{Q}(i)$ es un campo.

EJERCICIO 47. Sea K un campo y sea $a \in K$. Defina $a^1 := a$, $a^2 := a \cdot a$ y, para $n \in \mathbb{N}$ se define, inductivamente, $a^{n+1} := a^n \cdot a$. Demuestre que

$$a^{m+n} = a^m a^n, \quad \text{para } a \in K \text{ y } m, n \in \mathbb{N}.$$

EJERCICIO 48. Si $a \neq 0$ en K y $n \in \mathbb{N}$, defina $a^{-n} := (a^{-1})^n$. También se define, para $a \neq 0$, $a^0 = 1$. Generalice el ejercicio anterior demostrando que, si $a \neq 0$ en K y $m, n \in \mathbb{Z}$, entonces $a^{m+n} = a^m a^n$.

V.6.2 Campos ordenados

En el campo de números racionales se tiene un orden total $\leq$ compatible con las operaciones suma y producto del campo. El orden de $\mathbb{Q}$ se definió en términos de un subconjunto no vacío $P \subseteq \mathbb{Q}$, cuyos elementos decimos que son positivos y al conjunto P se le llamó una clase positiva. Las propiedades de este conjunto P son las siguientes: si K es un campo, una *clase positiva* en K es un subconjunto no vacío $P \subseteq K$ que satisface los axiomas:

(I) P es cerrado bajo la suma de K, es decir, si $a, b \in P$, entonces $a+b \in P$.

(II) P es cerrado bajo el producto de K, es decir, si $a, b \in P$, entonces $ab \in P$.

(III) P satisface la propiedad de *tricotomía*: si $a, b \in K$, entonces se cumple una y sólo una de las afirmaciones siguientes: $a \in P$, $a = 0$, $-a \in P$.

Si P es una clase positiva en un campo K, dados dos elementos $a, b \in K$, por la propiedad de tricotomía aplicada al elemento $b - a \in K$ se tiene que $b - a = 0$, $b - a \in P$ o $a - b \in P$; en el primer caso se tiene que $a = b$. Usando esto, se define un *orden parcial* $\leq$ en K mediante:

$$a \leq b \Leftrightarrow \begin{cases} a = b \\ \text{o} \\ b - a \in P \end{cases}$$

y se define $c \geq d \Leftrightarrow d \leq c$. Se define $a > b$ en K como $a > b \Leftrightarrow a \geq b$ y $a \neq b$. Similarmente se define $a < b$ en K. Note que esto fue lo que hicimos en $\mathbb{Q}$. Observe también que, dado un elemento $a \in K$ se tiene que $a > 0$ en K si y sólo si $a \in P$.

EJERCICIO 49. La relación $<$ de K satisface:

(1) $<$ es transitiva, *i.e.*, $a < b$ y $b < c$ implican que $a < c$.

(2) Compatibilidad con la suma: $a < b$ y $c \in K$ implican que $a + c < b + c$.

(3) Compatibilidad con el producto:

(I) $a < b$ y $c > 0 \Rightarrow ac < bc$.

(II) $a < b$ y $c < 0 \Rightarrow ac > bc$.

(4) Si $a > 0$ entonces $a^{-1} > 0$.

(5) Si $0 < a < b$ entonces $0 < b^{-1} < a^{-1}$.

(6) Si $a \neq 0$ en K, entonces $a^2 > 0$.

EJERCICIO 50. Si K es un campo ordenado, demuestre que la relación de orden $\leq$ es un orden total en K.

EJERCICIO 51. Si K es un campo ordenado, concluya del ejercicio anterior que si $a > b$, entonces $a > \dfrac{a+b}{2} > b$.

EJERCICIO 52. Si K es un campo ordenado, concluya del ejercicio anterior que si $a > 0$, entonces $a > \dfrac{a}{2} > 0$ y por lo tanto no existe elemento positivo menor en K.

EJERCICIO 53. Si K es un campo ordenado, concluya del ejercicio 51 anterior que si $a > b$, entonces existen infinitos elementos $x \in K$ tales que $a > x > b$.

EJERCICIO 54. Si K es un campo ordenado y si $ab > 0$, demuestre que $a > 0$ y $b > 0$ o $a < 0$ y $b < 0$.

EJERCICIO 55. En el campo $K := \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$ defina una clase positiva P, *i.e.*, dado $\alpha = a + b\sqrt{2} \in K$ defina cuándo $\alpha > 0$, *i.e.*, cuándo $\alpha \in P$. *Nota:* esta definición la tiene que hacer en términos del orden de $\mathbb{Q}$ y del elemento $\sqrt{2}$ únicamente.

Ejemplo 15. El campo $K = \{0, 1\}$ del ejemplo 14 no es un campo ordenado ya que si existiera una clase positiva $P \subseteq K$, las posibilidades para P son $P = \{0\}$ lo cual contradice la parte (III) de la definición para $a = 1$; la segunda posibilidad es $P = \{1\}$, pero ésta tampoco es posible ya que, por definición de suma en K, se tiene que $1+1 = 0 \notin P$ lo cual contradice (I) de la definición; la última posibilidad es $P = K$, pero esto tampoco es posible porque contradice (III) para $a = 1$ ya que $-a = 1$ por lo que 1 y -1 están ambos en P.

EJERCICIO 56. Si K es un campo ordenado, demuestre que si P es la clase positiva de K, entonces $1 \in P$.

EJERCICIO 57. Usando el ejercicio anterior demuestre que el campo $\mathbb{Q}(i)$ del ejercicio 46 no es un campo ordenado.

EJERCICIO 58. Si K es un campo ordenado y L es un campo contenido en K tal que las operaciones de L son las mismas operaciones que las de K restringidas a L y si P es una clase positiva en K, demuestre que $P \cap L$ es una clase positiva en L. Se sigue que L es un campo ordenado también.

Mostraremos a continuación que $\mathbb{Q}$ es el *menor campo ordenado*, *i.e.*, si K es cualquier campo ordenado, entonces K contiene a (una copia de) $\mathbb{Q}$:

PROPOSICIÓN V.19. *Si K es un campo ordenado, entonces existe una función inyectiva $\phi : \mathbb{Q} \to K$ que preserva las operaciones de K y $\mathbb{Q}$.*

Demostración. El campo K contiene al menos dos elementos: 0 y 1. Sabemos cómo multiplicarlos y consideremos ahora la suma $1 + 1$. Note que este elemento no puede ser 0, ya que si lo fuera el subconjunto $L = \{0, 1\} \subseteq K$ sería un campo contenido en K y por lo tanto sería un campo ordenado por el ejercicio 58, lo cual contradice el ejemplo 15. Observe ahora que $1 + 1$ tampoco puede ser 1, ya que la igualdad $1 + 1 = 1$ implica que $1 = 0$, en contradicción con el hecho de que $1 \neq 0$, como se pide en uno de los axiomas de campo. Se sigue que $1 + 1$ es un elemento distinto de 0 y 1 en K. Llamemos $2'$ al elemento $1 + 1$ de K y consideremos ahora al elemento $1 + 2' \in K$. En forma análoga a la anterior se prueba que $1 + 2'$ no es 0, 1 ni $2'$. Llamemos $3'$ al elemento $1 + 2'$. Por inducción se demuestra que, si $n \in \mathbb{N}$, entonces $n' \in K$. Hemos así definido una función $\phi : \mathbb{N} \to K$ mediante $\phi(1) = 1$ y $\phi(n) = n'$ y claramente ésta es inyectiva. Ahora, como K es un campo, y como para $n \in \mathbb{N}$ se tiene que $n' \in K$, entonces $-n' \in K$ y por lo tanto la función ϕ anterior se extiende a todo $\mathbb{Z}$, *i.e.*, se tiene una función inyectiva $\phi : \mathbb{Z} \to K$, y es un ejercicio fácil el probar que ϕ respeta las operaciones de $\mathbb{Z}$ y de K. Finalmente, si $n \in \mathbb{N}$, el elemento $n' \in K$ es diferente de 0 y por lo tanto tiene inverso multiplicativo $1/n' \in K$ y así, para $m' \in \mathbb{Z}$ se tiene que $m'/n' = m'(1/n') \in K$. Se sigue que ϕ se extiende a una función inyectiva $\phi : \mathbb{Q} \to K$ que respeta las operaciones de ambos campos. □

EJERCICIO 59. Demuestre que la función ϕ anterior en efecto preserva las operaciones de ambos campos, y es inyectiva.

El valor absoluto. Si K es un campo ordenado y si $a \in K$ con $a \neq 0$, entonces por tricotomía se tiene que $a > 0$ o $-a > 0$. Si $a \neq 0$, el *valor absoluto* $|a|$ de a es el elemento positivo del conjunto $\{a, -a\}$ y si $a = 0$ se define $|0| = 0$. En forma resumida,

$$|a| := \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0. \end{cases}$$

PROPOSICIÓN V.20. *Si K es un campo ordenado, el valor absoluto satisface las propiedades siguientes:*

1) $|-a| = |a|$.

2) $|ab| = |a||b|$.

3) $|a+b| \leq |a| + |b|$ (desigualdad del triángulo).

4) Si $c \geq 0$, *entonces* $|a| \leq c \Leftrightarrow -c \leq a \leq c$.

5) $-|a| \leq a \leq |a|$.

6) $||a| - |b|| \leq |a - b|$.

Demostración. Sólo probaremos (4) y (5) y dejamos los otros incisos como ejercicios para el lector. Para (4), si $|a| \leq c$, entonces $a \leq c$ y $-a \leq c$. De esta última desigualdad se sigue que $-c \leq a$, lo cual junto con la desigualdad $a \leq c$ nos da el resultado deseado: $-c \leq c \leq a$. Recíprocamente, si $-c \leq c \leq a$, entonces $a \leq c$ y $-c \leq a$. Esta última desigualdad implica que $-a \leq c$, lo cual junto con $a \leq c$ implica que $|a| \leq c$. Para (5), poniendo $c := |a| \geq 0$ en el inciso (4) el resultado se sigue. □

EJERCICIO 60. Demuestre las propiedades (1), (2), (3) y (6) de la proposición anterior.

EJERCICIO 61. Si K es un campo ordenado y $a_1, \ldots, a_n \in K$, demuestre que

$$|a_1 + \cdots + a_n| \leq |a_1| + \cdots + |a_n|.$$

EJERCICIO 62. Si K es un campo ordenado y $a^2 + b^2 = 0$, demuestre que $a = 0 = b$.

EJERCICIO 63. Si K es un campo ordenado y $a > 0$, demuestre que $(1+a)^n \geq 1 + na$ para toda $n \in \mathbb{N}$.

V.6.3 Campos ordenados completos

Como los números racionales $\mathbb{Q}$ forman un campo ordenado, los axiomas de campo y los axiomas de orden no son suficientes para caracterizar a los números reales y hay una propiedad importante de los números reales que no ha sido capturada en los axiomas anteriores, y para poder formularla necesitaremos un poco de terminología:

Supremos e ínfimos. Sea K un campo ordenado. Un subconjunto $A \subseteq K$ se dice que está *acotado por arriba* si existe un $c \in K$ tal que $x \leq c$ para todo $x \in A$. Al número c se le llama una *cota superior* de A. Similarmente, un conjunto $A \subseteq K$ se dice que está *acotado por abajo* si existe un $b \in K$ tal que $b \leq x$ para todo $x \in A$. Al número b se le llama una *cota inferior* de A.

Ejemplo 16. El conjunto $\{1/n \ : \ n \in \mathbb{N}\} \subseteq K$ está acotado superiormente por cualquier elemento $r \geq 1$ y está acotado inferiormente por cualquier elemento $s \leq 0$.

Ejemplo 17. El conjunto de elementos positivos de K, $P = K^+$ está acotado inferiormente por cualquier elemento $r \leq 0$, pero no está acotado superiormente.

(1) Si un conjunto $A \subseteq K$ está acotado superiormente, de todas sus cotas superiores podemos considerar la menor de ellas, digamos M. En otras palabras, este elemento $M \in K$ satisface:

(I) M es cota superior de A.

(II) M es la menor cota superior de A, *i.e.*, para cualquier cota superior C de A se tiene que $M \leq C$.

Una menor cota superior M de A, si existe, se llama un *supremo* de A y se denota por $M = \sup(A)$.

(2) Análogamente, si $A \subseteq K$ está acotado inferiormente, de todas sus cotas inferiores podemos considerar la mayor de ellas, digamos m. En otras palabras, este elemento $m \in K$ satisface:

(I) m es cota inferior de A.

(II) m es la mayor cota inferior de A, *i.e.*, para cualquier cota inferior c de A se tiene que $c \leq m$.

Una mayor cota inferior m de A, si existe, se llama un *ínfimo* de A y se denota por $m = \text{ínf}(A)$.

El uso de notaciones para supremos e ínfimos tiene sentido gracias a la unicidad de éstos, cuando existen:

LEMA V.21. *Sean K un campo ordenado y $A \subseteq K$. Si existe un supremo de A, éste es único. Similarmente para el ínfimo.*

Demostración. Supongamos que M_1 y M_2 son dos supremos de A. Como M_1 es supremo de A y M_2 es cota superior de A, entonces $M_1 \leq M_2$. Cambiando los papeles de M_1 y M_2 se tiene que $M_2 \leq M_1$. Se sigue que $M_1 = M_2$. Similarmente para el ínfimo. □

La proposición siguiente da una caracterización, que suele ser útil, del supremo (ínfimo) de un conjunto:

PROPOSICIÓN V.22. *Sea K un campo ordenado y sea $A \subseteq K$.*

1) *Una cota superior M de A es el supremo de A si y sólo si para toda $\varepsilon > 0$ en K existe $x \in A$ tal que $M - \varepsilon < x \leq M$.*

2) *Una cota inferior M de A es el ínfimo de A si y sólo si para toda $\varepsilon > 0$ en K existe $x \in A$ tal que $m \leq x < m + \varepsilon$.*

Demostración. Para (1), supongamos primero que $M = \sup(A)$ y supongamos que existe un $\varepsilon_0 > 0$ tal que $x \leq M - \varepsilon_0$ para todo $x \in A$. Se sigue que $M - \varepsilon_0$ es cota superior de A y como $M - \varepsilon_0 < M$ se tiene que M no es la menor cota superior de A, una contradicción. Recíprocamente, supongamos que M es una cota superior de A que satisface que para toda $\varepsilon > 0$ en K existe $x \in A$ tal que $M - \varepsilon < x \leq M$. Si M no fuera la menor cota superior de A, entonces existiría otra cota superior M_0 de A tal que $M_0 < M$. Pongamos $\varepsilon := M - M_0 \in K$; entonces $\varepsilon > 0$ y para este $\varepsilon > 0$ se tiene que, por hipótesis, existe $x \in A$ tal que $M - \varepsilon < x \leq M$, y como $M - \varepsilon = M - (M - M_0) = M_0$, entonces existe $x \in A$ tal que $M_0 < x \leq M$, en contradicción con el hecho de que M_0 es cota superior de A. □

EJERCICIO 64. Demuestre la parte (2) de la proposición anterior.

Ejemplo 18. Para el conjunto $A = \{1/n\}$ del ejemplo 16, se tiene que $\sup(A) = 1$ e $\inf(A) = 0$. Para el ínfimo se usó la parte (2) de la proposición anterior.

EJERCICIO 65. Si $A \subseteq K$ es un conjunto no vacío acotado por abajo, demuestre que el conjunto $-A := \{-x \ : \ x \in A\}$ está acotado por arriba. Demuestre que

$$\inf(A) = -\sup(-A).$$

EJERCICIO 66. Si $\emptyset \neq A \subseteq B \subseteq K$ y B es acotado por arriba y por abajo, demuestre que $\inf(B) \leq \inf(A) \leq \sup(A) \leq \sup(B)$.

EJERCICIO 67. Si K es un campo ordenado, $A \subseteq K$ y si $\lambda > 0$ en K, demuestre que

$$\sup\{\lambda a \ : \ a \in A\} = \lambda \cdot \sup(A) \qquad \text{e} \qquad \inf\{\lambda a \ : \ a \in A\} = \lambda \cdot \inf(A).$$

La proposición siguiente debe ser intuitivamente obvia:

PROPOSICIÓN V.23. *Sean K un campo ordenado y $A \subseteq K$ un conjunto no vacío con un número finito de elementos. Entonces,* $\sup(A)$ *existe y* $\sup(A) \in A$.

Demostración. Por inducción sobre el número $n = |A|$ de elementos de A.
(I) Si $n = 1$, entonces $A = \{a_1\}$ y $a_1 = \sup(A)$.
(II) Supongamos que la afirmación es verdadera para conjuntos con $\leq n$ elementos, y sea $A \subseteq K$ un conjunto con $n+1$ elementos. Fijemos cualquier elemento $a \in A$ y consideremos el conjunto $B = A - \{a\}$. Entonces, $|B| = n$ y, por hipótesis de inducción, $M' := \sup(B) \in B \subseteq A$. Por tricotomía $M' < a$ o $a \leq M'$. Si $a \leq M'$, entonces $\sup(A) = M' \in A$. Si $M' < a$, entonces $\sup(A) = a \in A$. □

COROLARIO V.24. *Si K es un campo ordenado y $A \subseteq \mathbb{Z} \subseteq K$ es un conjunto no vacío, acotado por arriba por un entero N_0, entonces* $\sup(A)$ *existe y* $\sup(A) \in A$.

Demostración. Si A contiene elementos ≥ 0, entonces $B := A \cap (\mathbb{N} \cup \{0\}) \neq \emptyset$. Ahora, como N_0 es cota superior de A, entonces también es cota superior de B y por lo tanto B tiene un número finito de elementos. Por la proposición anterior $\sup(B) \in B$ y es claro que $\sup(A) = \sup(B) \in B \subseteq A$, lo cual prueba el corolario en este caso.

Si A no contiene elementos > 0, como A está acotado por arriba por N_0, entonces $-A := \{-a \ : \ a \in A\}$ tiene sólo elementos ≥ 0 y así, por el principio del buen orden existe un elemento menor en $-A$, digamos n_0: entonces, $n_0 \leq -a$ y como $n_0 \in -A$, se sigue que $n_0 = \text{ínf}(-A)$. Ahora, como $n_0 \in -A$, entonces $n_0 = -m_0$ con $m_0 \in A$, por lo que $-m_0 = \text{ínf}(-A) = -\sup(A)$, la última igualdad por el ejercicio 65. Se sigue que $\sup(A) = m_0 \in A$. □

DEFINICIÓN V.25. Un campo ordenado K se dice que es *completo* si todo subconjunto no vacío $A \subseteq K$ que esté acotado por arriba tiene un supremo $\sup(A) \in K$. Un campo ordenado K es *arquimediano* si para todo $\alpha \in K$ existe un $N \in \mathbb{N}$ tal que $\alpha < N$.

Ejemplo 19. En el campo ordenado $\mathbb{Q}$ el conjunto

$$A = \{1, 1.4, 1.41, 1.414, 1.4142, \ldots\} \subseteq \mathbb{Q}$$

está acotado por arriba, por ejemplo por $1.5 \in \mathbb{Q}$: sin embargo no tiene un supremo en $\mathbb{Q}$. De hecho, el lector puede tener la sospecha de que $\sup(A) = \sqrt{2}$ y ya sabe que $\sqrt{2} \notin \mathbb{Q}$.

Probaremos a continuación que todo campo ordenado completo es arquimediano, pero antes recordamos que $\mathbb{Q}$ es arquimediano por (IV.11) y el ejercicio 12 del capítulo IV. Así, el ejemplo 19 anterior nos dice que $\mathbb{Q}$ es un campo ordenado arquimediano no completo.

EJERCICIO 68. Si K es un campo arquimediano y $A \subseteq \mathbb{Z} \subseteq K$ es un conjunto no vacío acotado por arriba, demuestre que $\sup(A)$ existe y $\sup(A) \in A$. *Sugerencia:* use que K es arquimediano para acotar A superiormente por un entero y entonces aplique el corolario anterior.

La conclusión de este ejercicio sigue siendo válida si K es completo:

PROPOSICIÓN V.26. *Si K es un campo ordenado completo y $A \subseteq \mathbb{Z} \subseteq K$ es un conjunto no vacío acotado por arriba. entonces* $\sup(A)$ *existe y* $\sup(A) \in A$.

Demostración. Como K es completo, entonces $\sup(A)$ existe. Sea $M = \sup(A) \in K$ y supongamos que $M \notin A$. Entonces, para toda $a \in A$ se tiene que $a < M$. Entonces, por la proposición (V.22)(1), para todo $\varepsilon > 0$ en K existe un $x \in A \subseteq \mathbb{Z}$ tal que $M - \varepsilon < x < M$. En particular, para $\varepsilon = 1$ existe un $a' \in A \subseteq \mathbb{Z}$ tal que $M - 1 < a' < M$. También, ahora para $\varepsilon = M - a' > 0$ existe un $a'' \in A \subseteq \mathbb{Z}$ tal que $M - (M - a') < a'' < M$; pero $M - (M - a') = a'$, por lo que

$$M - 1 < a' < a'' < M,$$

es decir, se tienen dos enteros a', a'' que difieren por menos de 1, lo cual es imposible. Se sigue que $\sup(A) \in A$. □

Usando esta proposición, probaremos que todo campo ordenado completo es arquimediano:

TEOREMA V.27. *Todo campo ordenado completo K es arquimediano.*

Demostración. Si K fuera no arquimediano, entonces existiría un $\alpha \in K$ tal que $n \leq \alpha$, para todo $n \in \mathbb{N}$. Ahora, por la proposición anterior aplicada a $A = \mathbb{N}$, el elemento $\alpha \in K$ es cota superior de $\mathbb{N}$ y por lo tanto $\sup(\mathbb{N}) \in \mathbb{N}$, *i.e.*, existe un natural $N \in \mathbb{N}$ tal que $n \leq N$, para todo $n \in \mathbb{N}$. Pero, para $n = N + 1 \in \mathbb{N}$ se tendría entonces que $n = N + 1 \leq N$, una contradicción. □

En este momento el lector podría preguntarse por un ejemplo de un campo ordenado completo y es tiempo de decirle que hemos llegado al punto donde la existencia de un tal campo debe ser asumida: denotaremos por $\mathbb{R}$ a un campo ordenado completo; los elementos de $\mathbb{R}$ se llaman *números reales*. Es importante resaltar que lo que distingue a $\mathbb{R}$ de $\mathbb{Q}$ es la propiedad de que en $\mathbb{R}$ todo conjunto no vacío acotado por arriba tiene un supremo en $\mathbb{R}$. Cuando el lector se sienta suficientemente seguro, se le sugiere que regrese al inicio del capítulo V a estudiar una de las construcciones del campo $\mathbb{R}$ y, al final del capítulo, en V.15, se demuestra la unicidad de un tal campo ordenado completo.

EJERCICIO 69. Si K es un campo ordenado arquimediano, demuestre que si $0 < a < b$ en K, entonces existe $n \in \mathbb{N}$ tal que $na > b$.

EJERCICIO 70. Si K es un campo ordenado arquimediano, demuestre que si $a > 0$ y $b > 0$ en K, entonces existe $n \in \mathbb{N}$ tal que $na > b$.

EJERCICIO 71. Si K es un campo ordenado arquimediano, demuestre que si $a > 0$, entonces existe $n \in \mathbb{N}$ tal que $n - 1 \leq a < n$. *Sugerencia*: use la propiedad arquimediana de K y el principio del buen orden en $\mathbb{N}$.

EJERCICIO 72. Si K es un campo ordenado arquimediano, demuestre que si $a > 0$, entonces existe $n \in \mathbb{N}$ tal que $0 \leq \frac{1}{n} < a$.

Este ejercicio nos dice que en un campo ordenado arquimediano existen racionales positivos arbitrariamente pequeños (recuerde que $\mathbb{Q} \subseteq K$).

EJERCICIO 73. Usando el ejercicio anterior, demuestre que si K es un campo ordenado arquimediano, entonces los racionales son densos en K, *i.e.,* si $a < b$ en K, entonces existe un racional $r \in \mathbb{Q} \subseteq K$ tal que $a < r < b$.

EJERCICIO 74. Este ejercicio nos dice que, si K es un campo ordenado arquimediano, y existe un irracional en K, *i.e.,* $\alpha \in K - \mathbb{Q}$, entonces existen irracionales positivos arbitrariamente pequeños. Es decir, si existe un irracional $\alpha \in K$ (al que, sin perder generalidad, podemos suponer positivo), demuestre que existe $n \in \mathbb{N}$ tal que $0 < \frac{\alpha}{n} < \alpha$ y α/n es irracional.

EJERCICIO 75. Usando el ejercicio anterior, demuestre que si K es un campo ordenado arquimediano y existe un irracional en K, entonces los irracionales son densos en K, *i.e.,* si $a < b$ en K, entonces existe un irracional $\xi \in K$ tal que $a < \xi < b$.

EJERCICIO 76. Si K es un campo ordenado arquimediano, demuestre que para todo $\varepsilon > 0$ en K existe $n \in \mathbb{N}$ tal que $\dfrac{1}{2^n} < \varepsilon$. *Sugerencia:* en algún punto usará que $2^n > n$, para toda $n \in \mathbb{N}$, lo cual se puede demostrar por inducción.

V.6.4 Bibliografía

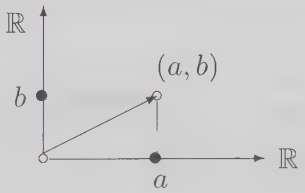
[1] Rudin, W., *Principles of Mathematical Analysis*, McGraw-Hill, Nueva York, 1964.

VI. EL CAMPO DE NÚMEROS COMPLEJOS

Los números reales los podemos sumar, restar, multiplicar y dividir (excepto por 0), podemos obtener las raíces de reales no negativos y toda sucesión de Cauchy converge en $\mathbb{R}$. Sin embargo, no existen en $\mathbb{R}$ las raíces pares de números reales negativos, por ejemplo, $\sqrt{-1} \notin \mathbb{R}$, es decir, no existe un número real $x \in \mathbb{R}$ tal que $x^2 = -1$, *i.e.*, la ecuación $x^2 + 1 = 0$ no tiene soluciones en $\mathbb{R}$. Ecuaciones como la anterior llevaron a la introducción de una nueva clase de números que originalmente se llamaban imaginarios (reflejando de alguna manera la inseguridad con que los matemáticos originalmente los trataban) y actualmente llamamos *números complejos* y veremos que contienen al campo de los números reales. La construcción del conjunto de los números complejos $\mathbb{C}$ y la demostración de que forman un campo, también completo en el sentido de que toda sucesión de Cauchy en $\mathbb{C}$ converge en $\mathbb{C}$, es más sencilla que las de los campos considerados anteriormente.

VI.1 El campo de números complejos

Como conjunto, $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ es el producto cartesiano de $\mathbb{R}$ consigo mismo. Así, $\mathbb{C} := \{(a, b) \ : \ a, b \in \mathbb{R}\}$. Podemos entonces representar estos pares (a, b) como puntos en el plano cartesiano $\mathbb{R} \times \mathbb{R}$ o mejor aún podemos pensar al número complejo (a, b) como una flecha (segmento dirigido) con origen $(0, 0)$ y extremo final el punto (a, b):



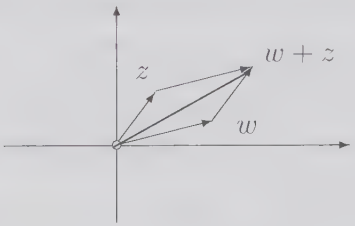
Usaremos letras como u, v, w, z para representar a números complejos.

Las operaciones aritméticas en $\mathbb{C}$ se definen como sigue:

SUMA. Dados dos números complejos $z = (a, b)$ y $w = (c, d)$ en $\mathbb{C}$ se suman componente a componente:

$$z + w = (a, b) + (c, d) := (a + c, b + d) \in \mathbb{C}.$$

Gráficamente esto se interpreta considerando a los complejos z, w como segmentos dirigidos en el plano $\mathbb{C}$ de tal forma que la suma $z + w$ es la diagonal del paralelogramo que determinan z y w:



Es fácil verificar que esta operación satisface los axiomas para la suma en un campo, por ejemplo el *neutro aditivo* es el complejo $0 := (0, 0)$ ya que para todo $z = (a, b) \in \mathbb{C}$ se tiene que

$$z + 0 = (a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = z$$

donde en la penúltima igualdad se usó que $a + 0 = a$ y $b + 0 = b$ en $\mathbb{R}$. Para la existencia de *inversos aditivos* observe que si $z = (a, b) \in \mathbb{C}$ entonces su inverso aditivo es el complejo $-z := (-a, -b)$ ya que

$$z + (-z) = (a, b) + (-a, -b) = (a - a, b - b) = (0, 0) = 0,$$

la penúltima igualdad porque $a - a = 0$ y $b - b = 0$ en $\mathbb{R}$.

EJERCICIO 1. Demuestre la asociatividad y conmutatividad de la suma en $\mathbb{C}$.

PRODUCTO. A primera vista la forma natural de definir un producto en $\mathbb{C}$ es como con la suma: componente a componente: $(a, b) \cdot (c, d) = (ac, bd)$, pero a pesar de que la asociatividad y conmutatividad del producto se verifican fácilmente con esta definición, observamos que en este caso el neutro multiplicativo debe ser el complejo $(1, 1)$ y entonces ya estamos en problemas con la existencia de inversos multiplicativos para los complejos $z \neq 0$: por ejemplo, el complejo $(2, 0) \neq (0, 0)$ pero $(2, 0)$ no tiene inverso multiplicativo

con respecto a este producto. Como queremos que $\mathbb{C}$ sea un campo debemos entonces definir el producto en una forma diferente. La definición que daremos parecerá poco natural al principio, pero veremos un poco después que con la notación adecuada (de hecho, la notación histórica) es de hecho muy natural. La definición es la siguiente: dados dos complejos $z = (a, b)$ y $w = (c, d)$, su producto es:

$$z \cdot w = (a, b)(c, d) := (ac - bd, ad + bc) \in \mathbb{C}.$$

Esta definición no tiene una interpretación geométrica natural como con la suma. Más tarde, usando la representación polar de un número complejo, daremos una interpretación geométrica del producto de complejos.

TEOREMA VI.1. *Con las operaciones anteriores* $(\mathbb{C}, +, \cdot)$ *es un campo.*

Demostración. Ya verificamos las propiedades de la suma. Para el producto, la *asociatividad, conmutatividad y distributividad* las dejamos como ejercicio. Para la existencia del *neutro multiplicativo*, queremos un complejo $(x, y) \in \mathbb{C}$ tal que para todo complejo (a, b) se tenga que

$$(*) \qquad (a, b)(x, y) = (a, b).$$

Observamos ahora que si $(a, b) = (0, 0)$ la igualdad $(*)$ es cierta no importa quién sea (x, y). Supongamos entonces que $(a, b) \neq (0, 0)$; entonces $a \neq 0$ o $b \neq 0$ y por lo tanto $a^2 + b^2 \neq 0$ en $\mathbb{R}$. Ahora, desarrollando el producto en la igualdad $(*)$:

$$(a, b)(x, y) = (ax - by, ay + bx) = (a, b)$$

por lo que, igualando componentes, se obtiene un sistema de ecuaciones lineales en dos incógnitas x, y con coeficientes reales:

$$\begin{aligned} ax - by &= a \\ bx + ay &= b. \end{aligned}$$

Observamos que este sistema de ecuaciones tiene solución única ya que el determinante del sistema es

$$\Delta := \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \neq 0$$

y esta solución la obtenemos ya sea eliminando variables o usando determinantes:

$$x = 1 \qquad \& \qquad y = 0,$$

por lo que $(x, y) = (1, 0)$ debe ser el *neutro multiplicativo* de $\mathbb{C}$. Usaremos la notación $1 = (1, 0) \in \mathbb{C}$.

Para la existencia de *inversos multiplicativos*, dado un complejo $z = (a, b) \neq 0$ queremos otro complejo $(x, y) \in \mathbb{C}$ tal que $(a, b)(x, y) = (1, 0) = 1$. Escribiendo las ecuaciones lineales correspondientes como arriba y resolviendo este sistema, se obtiene que:

$$x = \frac{a}{a^2 + b^2}, \qquad y = \frac{-b}{a^2 + b^2}$$

de tal forma que el inverso multiplicativo de $z \neq 0$ es el complejo

$$z^{-1} := \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right),$$

y de hecho se verifica directamente que $zz^{-1} = 1$. □

EJERCICIO 2. Demuestre la asociatividad, conmutatividad y distributividad del producto en $\mathbb{C}$.

Como en cualquier campo, en $\mathbb{C}$ se tienen las operaciones de *resta* y *división*:

Resta. Dados complejos $z, w \in \mathbb{C}$ se define

$$z - w := z + (-w)$$

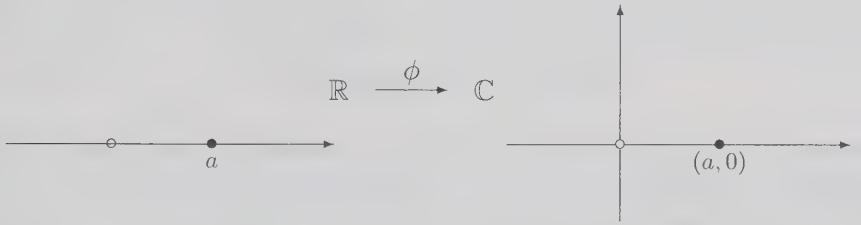
(sumando el inverso aditivo de w).

División. Dados complejos $z, w \in \mathbb{C}$ con $w \neq 0$, se define

$$\frac{z}{w} := z \cdot (w^{-1})$$

(producto por el inverso multiplicativo de w).

Así como $\mathbb{Q} \subseteq \mathbb{R}$, se tiene que $\mathbb{R}$ está incluido naturalmente en $\mathbb{C}$. Recordemos que los números reales se pueden representar geométricamente como puntos en una recta, la recta real, y esta recta la podemos incluir en el plano complejo de varias formas, por ejemplo, como uno de los ejes coordenados; escogemos una de estas inmersiones de $\mathbb{R}$ en $\mathbb{C}$ de tal forma que se preserven las operaciones de ambos campos y esta inmersión es la que identifica la recta real $\mathbb{R}$ con el eje horizontal de $\mathbb{C}$, es decir, se define la función $\phi : \mathbb{R} \to \mathbb{C}$ mediante $\phi(a) := (a, 0)$ para $a \in \mathbb{R}$:



Ejercicio 3. Demuestre que ϕ es inyectiva y preserva las operaciones de $\mathbb{R}$ y $\mathbb{C}$. De esta forma ϕ identifica al número real $a \in \mathbb{R}$ con el número complejo $(a, 0)$. Algunas veces omitimos a la ϕ de esta notación y escribimos $a = (a, 0)$.

Ejercicio 4. Demuestre que $\phi(0) = 0$ y $\phi(1) = 1$, donde en los lados izquierdos tenemos al 0 y 1 de $\mathbb{R}$ y en los lados derechos son los de $\mathbb{C}$. Gracias a esta propiedad no existe confusión al denotar con los mismos símbolos a los ceros y unos de $\mathbb{R}$ y $\mathbb{C}$.

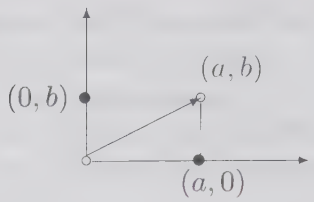
Ejercicio 5. Si $a \in \mathbb{R}$ demuestre que $\phi(-a) = -\phi(a)$. Y si $a \neq 0$, demuestre que $\phi(a^{-1}) = \phi(a)^{-1}$.

Como la recta real $\mathbb{R}$ ha sido identificada con el eje horizontal de $\mathbb{C}$, llamaremos a este eje el *eje real* de $\mathbb{C}$. Por razones históricas al eje vertical de $\mathbb{C}$ se le llama el *eje imaginario*.

Observemos ahora que dado cualquier número complejo $z = (a, b) \in \mathbb{C}$, lo podemos escribir como

$$z = (a, b) = (a, 0) + (0, b) \tag{1}$$

con $(a, 0)$ en el eje real y $(0, b)$ en el eje imaginario:



Recordemos ahora que $(a, 0) = a$ por la identificación que hicimos antes. Para el otro sumado $(0, b)$, observemos que en el eje real se tiene al neutro multiplicativo $1 = (1, 0)$ y si escogemos en el eje imaginario al complejo $i := (0, 1) \in \mathbb{C}$ al que podemos llamar la *unidad imaginaria* observamos que

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1,$$

es decir, $i^2 = -1$ por lo que $i \in \mathbb{C}$ es una raíz cuadrada de -1, algo que ciertamente no sucede en $\mathbb{R}$ porque el cuadrado de cualquier real es ≥ 0. Notemos ahora que para todo complejo $(0, b)$ en el eje imaginario se tiene que

$$(0, b) = (b, 0)(0, 1) = bi$$

de tal forma que todo número en el eje imaginario es un múltiplo real del complejo i. Substituyendo estas observaciones en la igualdad (1) de arriba vemos que todo número complejo $z = (a, b) \in \mathbb{C}$ se puede escribir de la forma:

$$z = (a, 0) + (0, b) = a + bi$$

con $a, b \in \mathbb{R}$ y donde el complejo i satisface que $i^2 = -1$. El número real a se llama la *parte real* del complejo $z = a + bi$ y el número real b se llama la *parte imaginaria* del complejo $z = a + bi$. Se suele usar la notación

$$a = \mathrm{Re}(z) \quad \text{y} \quad b = \mathrm{Im}(z).$$

Con esta nueva notación las operaciones de suma y producto en $\mathbb{C}$ se vuelven:

Suma. Dados dos complejos $z = a + bi$ y $w = c + di$, su suma es:

$$z + w = (a + bi) + (c + di) = (a + b) + (b + d)i,$$

es decir, se suman las partes reales y aparte se suman las partes imaginarias.

Producto. Dados dos complejos $z = a + bi$ y $w = c + di$, su producto es:

$$\begin{aligned} zw &= (a+bi)(c+di) \\ &= ac + adi + bci + bdi^2 && \text{usando la distributividad} \\ &= ac + adi + bci - bd && \text{porque } i^2 = -1 \\ &= (ac - bd) + (ad + bc)i && \text{separando partes reales de imaginarias.} \end{aligned}$$

Observamos que con esta notación, la fórmula para el producto de dos complejos es entonces natural.

Antes de hacer unos ejemplos con las operaciones de $\mathbb{C}$ introduciremos un par de conceptos asociados a números complejos:

Conjugación. Dado un número complejo $z = a + bi$ se define su *conjugado* $\overline{z} := a - bi$ cambiando el signo de la parte imaginaria de z. Las propiedades siguientes de la conjugación son fáciles de demostrar:

EJERCICIO 6. Sean $w, z \in \mathbb{C}$. Demuestre que:

(1) $\overline{\overline{z}} = z$.

(2) $\overline{z + w} = \overline{z} + \overline{w}$.

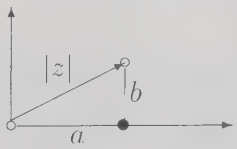
(3) $\overline{zw} = \overline{z}\,\overline{w}$.

(4) Si $z \neq 0$, entonces $\overline{(z^{-1})} = (\overline{z})^{-1}$.

(5) Si $z \neq 0$, entonces $\overline{\left(\dfrac{w}{z}\right)} = \dfrac{\overline{w}}{\overline{z}}$.

(6) $z \in \mathbb{R} \Leftrightarrow \overline{z} = z$ (es decir, un número complejo es un número real si y sólo si es igual a su conjugado).

Módulo. Dado un número complejo $z = a+bi$ pensándolo como un segmento dirigido en el plano podemos considerar su longitud:



y a esta longitud le llamamos el *módulo* del complejo z y lo denotamos $|z|$.

En la figura anterior observamos que se tiene un triángulo rectángulo con catetos a, b y con hipotenusa el módulo $|z|$, de tal forma que, por el teorema de Pitágoras

$$|z|^2 = a^2 + b^2$$

con $a^2 + b^2 \geq 0$ en $\mathbb{R}$, por lo que $|z| = +\sqrt{a^2 + b^2}$ y así el módulo $|z|$ es un número real positivo.

Observemos ahora que si $z = a + bi$ entonces

$$z \cdot \overline{z} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2 = |z|^2,$$

por lo que

$$|z| = +\sqrt{z \cdot \overline{z}}.$$

Usando esta expresión para el módulo de un complejo, se verifican fácilmente las propiedades siguientes:

EJERCICIO 7. Sean $w, z \in \mathbb{C}$. Demuestre que:

(1) $|z| = |\overline{z}|$.

(2) $|zw| = |z||w|$.

(3) Si $z \neq 0$, entonces $\left|\dfrac{w}{z}\right| = \dfrac{|w|}{|z|}$.

(4) $|z + w| \leq |z| + |w|$ (la desigualdad del triángulo).

Veamos ahora cómo estos dos conceptos nos facilitan ciertas operaciones en $\mathbb{C}$, por ejemplo supongamos que queremos dividir un complejo w entre un complejo $z \neq 0$. Para esto escribamos:

$$(*) \qquad \frac{w}{z} = \frac{w\overline{z}}{z\overline{z}},$$

es decir, multipliquemos la fracción $\dfrac{w}{z}$ que queremos calcular por $1 = \dfrac{\overline{z}}{\overline{z}}$ de tal forma que no varía. Notamos, sin embargo, que en el lado derecho de $(*)$ se tiene en el denominador un número real: $z\overline{z} = |z|^2$ y de esta manera el lado derecho es fácil de calcular. Un ejemplo ilustra esto:

Ejemplo 1. Si $z = 2 + 3i$ y $w = 4 - i$ calculemos el cociente w/z y al final escribámoslo en la forma $a + bi$. Esto se hace como se indicó arriba:

$$\frac{4-i}{2+3i} = \frac{(4-i)(\overline{2+3i})}{(2+3i)(\overline{2+3i})} = \frac{(4-i)(2-3i)}{(2+3i)(2-3i)} = \frac{8-12i-2i+3i^2}{4+9}$$
$$= \frac{5-14i}{13} = \frac{5}{13} - \frac{14}{13}\,i.$$

EJERCICIO 8. Si $z = a + bi$, demuestre que

$$\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z})$$
$$\mathrm{Im}(z) = \frac{1}{2i}(z - \overline{z}).$$

EJERCICIO 9. Considere el conjunto $S \subseteq \mathbb{C}$ definido por:

$$S := \{z \in \mathbb{C} \ : \ |z| = 1\}.$$

a) Demuestre que S es cerrado bajo productos, es decir, demuestre que si $u, v \in S$ entonces $uv \in S$.

b) Demuestre que S es cerrado bajo inversos, es decir, demuestre que si $u \in S$ entonces $u^{-1} \in S$.

c) Grafique S en el plano complejo $\mathbb{C}$.

EJERCICIO 10. Haga las operaciones indicadas y al final exprese el resultado en la forma $a + bi$:

a) $(3 + 2i) + (5 - 3i)$.

b) $(5 + 7i) - (4 - 2i)$.

c) $3i - (-7 + 2i)$.

d) $5 + (\frac{1}{2} - 3i)$.

e) $(2 + 3i)(4 - 2i)$.

f) $\dfrac{3 + 4i}{5 + 2i}$.

g) $\dfrac{4}{2-3i}$.

h) $\dfrac{(2+i)(3+2i)}{1-i}$.

i) $(2+i)^5$.

j) $\left(-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}\,i\right)^4$.

k) i^n para $n=1,2,3,\ldots$

EJERCICIO 11. Calcule el módulo de los siguientes complejos:

a) $w=2-i$.

b) $w=\dfrac{3-i}{\sqrt{2}+3i}$.

c) $w=(1+i)^6$.

d) $w=i^{203}$.

Observación. Es importante notar que *en el campo* $\mathbb{C}$ *no puede existir una relación de orden compatible con las operaciones de* $\mathbb{C}$, ya que cualquier clase positiva P (en el caso que existiera) debe contener al 1 de $\mathbb{C}$ y al cuadrado de cualquier complejo $\neq 0$. Sin embargo, para el complejo $z=i$ se tiene que $i^2=-1$ que no puede estar en la (supuesta) clase positiva P de $\mathbb{C}$, por tricotomía, ya que $1\in P$.

Completez del campo $\mathbb{C}$. En el campo de números complejos $\mathbb{C}$ podemos definir sucesiones en forma similar a como se hizo en $\mathbb{Q}$ y $\mathbb{R}$: una *sucesión* en $\mathbb{C}$ es una función $z:\mathbb{N}\to\mathbb{C}$. Si $n\in\mathbb{N}$, a su imagen bajo $z:\mathbb{N}\to\mathbb{C}$ la denotamos como $z(n)=z_n$. Como es usual, también usamos la notación $\{z_n\}$ para una sucesión en $\mathbb{C}$.

Usando el módulo $|z_n|$ de los números complejos $z_n\in\mathbb{C}$ podemos definir el concepto de límite de una sucesión: dada una sucesión $\{z_n\}$ en $\mathbb{C}$, diremos que el complejo $z\in\mathbb{C}$ es *límite* de $\{z_n\}$ si $\forall\,\varepsilon>0$ en $\mathbb{R}$, existe $N\in\mathbb{N}$ tal que $|z_n-z|<\varepsilon$ siempre que $n>N$. Si la sucesión $\{z_n\}$ tiene un límite en $\mathbb{C}$, diremos que $\{z_n\}$ es *convergente*. Similarmente, se dice que la sucesión $\{z_n\}$ de $\mathbb{C}$ es una *sucesión de Cauchy* si $\forall\,\varepsilon>0$ en $\mathbb{R}$, existe $N\in\mathbb{N}$ tal que $|z_m-z_n|<\varepsilon$ siempre que $m,n\geq N$.

EJERCICIO 12. Para sucesiones $\{z_n\}$ en $\mathbb{C}$, enuncie y demuestre las propiedades correspondientes a (V.1), (V.2), (V.3) y (V.4).

EJERCICIO 13. Si $z = a + bi \in \mathbb{C}$, con $a, b \in \mathbb{R}$, demuestre que $|a| \leq |z|$ y $|b| \leq |z|$, donde a la izquierda se tiene el valor absoluto de $\mathbb{R}$, y a la derecha se tiene el módulo del complejo $|z|$.

EJERCICIO 14. Si $\{z_n\}$ es una sucesión en $\mathbb{C}$, escribiendo cada $z_n = a_n + b_n\, i$, con $a_n, b_n \in \mathbb{R}$, se tienen las sucesiones $\{a_n\}$ y $\{b_n\}$ en $\mathbb{R}$. Recíprocamente, dadas las sucesiones $\{a_n\}$ y $\{b_n\}$ en $\mathbb{R}$, definiendo $z_n = a_n + b_n\, i$, se tiene la sucesión $\{z_n\}$ en $\mathbb{C}$.

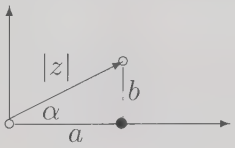
a) Demuestre que $\{z_n\}$ es de Cauchy si y sólo si $\{a_n\}$ y $\{b_n\}$ son de Cauchy en $\mathbb{R}$.

b) Demuestre que $\{z_n\}$ converge a $z = a + bi \in \mathbb{C}$ si y sólo si $\{a_n\}$ converge a a y $\{b_n\}$ converge a b en $\mathbb{R}$.

EJERCICIO 15. Concluya que $\mathbb{C}$ es un campo completo.

VI.2 FORMA POLAR DE UN NÚMERO COMPLEJO

Considere un número complejo $z = a + bi \in \mathbb{C}$:



(1) Si $z \neq 0$, definimos su *argumento* como el ángulo α entre el semieje real positivo y el segmento dirigido determinado por α (véase la figura anterior). Como es usual, el ángulo se considera positivo si se mide en sentido contrario al de las manecillas del reloj y negativo en caso contrario. Observe también que el argumento α no es único, *i.e.*, la asignación $z \mapsto \alpha$ no es una función ya que podemos reemplazar α por $\alpha + 2\pi$ o, en general, por $\alpha + 2k\pi$, para cualquier $k \in \mathbb{Z}$. Al complejo $z = 0 \in \mathbb{C}$ no le asignamos un argumento.

(2) Ahora, si $z \neq 0$ y $z = a + bi$, consideremos el triángulo formado por a, b y $|z|$ (véase la figura anterior) donde observamos que $|z| \neq 0$; se tiene entonces que:

$$\cos(\alpha) = \frac{a}{|z|} \quad \text{por lo que } a = |z|\cos(\alpha),$$
$$\operatorname{sen}(\alpha) = \frac{b}{|z|} \quad \text{por lo que } b = |z|\cos(\alpha)$$

y por lo tanto

$$z = a + bi = |z|\cos\alpha + i\,|z|\operatorname{sen}\alpha,$$

i.e.,

$$z = |z|(\cos\alpha + i\ \operatorname{sen}\alpha)$$

y a esta representación de z la llamamos la *forma polar* del complejo $z \neq 0$.

Observación. Para cambiar de la forma $z = a + bi \neq 0$ a la forma polar se necesitan:

(1) El módulo de z, el cual se obtiene con $|z| = \sqrt{a^2 + b^2}$.

(2) El argumento α de z. Para calcularlo observamos que como $z = a + bi \neq 0$, entonces $a \neq 0$ o $b \neq 0$. Si $a \neq 0$, entonces $\alpha = \arctan(b/a)$, y si $b \neq 0$, entonces $\alpha = \operatorname{arccot}(a/b)$.

Con estos datos se tiene que $z = |z|(\cos\alpha + i\ \operatorname{sen}\alpha)$.

Observación. Para cambiar de la forma polar $z = |z|(\cos\alpha + i\ \operatorname{sen}\alpha)$ a la forma $a + bi$ se calculan $\cos(\alpha)$ y $\operatorname{sen}(\alpha)$ y se multiplican por $|z|$.

Ejemplo 2. Encuentre la representación polar de $z = 2 + 2i$. En este ejemplo $|z| = \sqrt{2^2 + 2^2} = 2\sqrt{2}$ y $\tan(\alpha) = 2/2 = 1$ por lo que $\alpha = \arctan(1) = \pi/4 = 45°$. Se sigue que

$$z = |z|(\cos\alpha + i\ \operatorname{sen}\alpha) = 2\sqrt{2}(\cos\pi/4 + i\ \operatorname{sen}\pi/4).$$

Ejemplo 3. Escriba en la forma $a + bi$ el complejo $w = 4(\cos\pi/3 + i\ \operatorname{sen}\pi/3)$. Esto es directo:

$$w = 4(\cos\pi/3 + i\ \operatorname{sen}\pi/3) = 4\left(\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right) = 2 + 2\sqrt{3}i.$$

La representación polar de un número complejo es útil para calcular potencias o raíces. Para esto, consideraremos primero el producto de números complejos dados en forma polar: dados dos números complejos en forma polar:

$$w = |w|(\cos\alpha + i\ \operatorname{sen}\alpha), \quad z = |z|(\cos\beta + i\ \operatorname{sen}\beta),$$

calculemos su producto:

$$\begin{aligned} wz &= |w|[\cos\alpha + i\ \operatorname{sen}\alpha]|z|[\cos\beta + i\ \operatorname{sen}\beta] \\ &\quad - |w_1|z|[\cos\alpha + i\ \operatorname{sen}\alpha][\cos\beta + i\ \operatorname{sen}\beta] \\ &= |w||z|[\cos\alpha\cos\beta + i\ \cos\alpha\operatorname{sen}\beta + i\ \operatorname{sen}\alpha\cos\beta + i^2\operatorname{sen}\alpha\operatorname{sen}\beta] \\ &= |w||z|[(\cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta) + i\ (\operatorname{sen}\alpha\cos\beta + \cos\alpha\operatorname{sen}\beta)] \\ &= |w||z|[\cos(\alpha+\beta) + i\ \operatorname{sen}(\alpha+\beta)], \end{aligned}$$

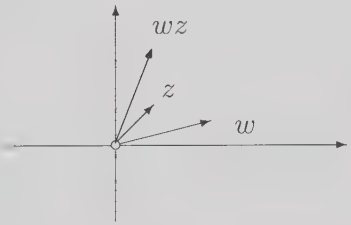
(la última igualdad se obtiene usando identidades trigonométricas para el seno y coseno de la suma de dos ángulos). Resumiendo, se tiene que

$$(*) \qquad wz = |w||z|[\cos(\alpha+\beta) + i\ \operatorname{sen}(\alpha+\beta)].$$

La igualdad anterior nos dice que para multiplicar dos complejos en forma polar:

(1) Se multiplican los módulos correspondientes.
(2) Se suman los argumentos.

De paso observamos que lo anterior nos da una interpretación geométrica del producto de dos números complejos:



Esta fórmula para el producto de dos complejos en forma polar nos será muy útil para calcular potencias z^n con $n \geq 0$ entero, de un número complejo $z \neq 0$. En efecto, si $z = |z|(\cos\alpha + i\ \operatorname{sen}\alpha)$, entonces

$$z^n = (|z|(\cos\alpha + i\ \operatorname{sen}\alpha))^n = |z|^n[\cos(n\alpha) + i\ \operatorname{sen}(n\alpha)]$$

donde la última igualdad se demuestra fácilmente por inducción sobre n usando la fórmula para el producto $(*)$ de arriba.

EJERCICIO 16. Demuestre la afirmación anterior.

La fórmula anterior para z^n con $n \geq 0$ también es válida para $n < 0$. Para probar esto observe que si $z \neq 0$ y $n < 0$, entonces $z^n = (z^{-1})^{-n}$ con $-n > 0$ y si $z = |z|(\cos\alpha + i\ \mathrm{sen}\,\alpha)$ entonces

$$z^{-1} = |z|^{-1}(\cos(-\alpha) + i\ \mathrm{sen}(-\alpha))$$

ya que, como el inverso multiplicativo de z es único, es suficiente observar que:

$$\begin{aligned} z|z|^{-1}[\cos(-\alpha) + i\ \mathrm{sen}(-\alpha)] &= |z|[\cos\alpha + i\ \mathrm{sen}\,\alpha]|z|^{-1}[\cos(-\alpha) + i\ \mathrm{sen}(-\alpha)] \\ &= |z||z|^{-1}[\cos\alpha + i\ \mathrm{sen}\,\alpha][\cos(-\alpha) + i\ \mathrm{sen}(-\alpha)] \\ &= 1[\cos(\alpha - \alpha) + i\ \mathrm{sen}(\alpha - \alpha)] \\ &= 1[\cos 0 + i\ \mathrm{sen}\,0] \\ &= 1, \end{aligned}$$

i.e., $|z|^{-1}[\cos(-\alpha) + i\ \mathrm{sen}(-\alpha)] = z^{-1}$. Usando esta fórmula para el inverso multiplicativo de un complejo se sigue que si $z \neq 0$ y $n < 0$:

$$\begin{aligned} z^n &= (z^{-1})^{-n} \quad \text{donde } -n > 0 \\ &= \left(|z|^{-1}(\cos(-\alpha) + i\ \mathrm{sen}(-\alpha))\right)^{-n} \\ &= \left(|z|^{-1}\right)^{-n}[\cos(-n(-\alpha)) + i\ \mathrm{sen}(-n - \alpha)] \\ &= |z|^n[\cos(n\alpha) + i\ \mathrm{sen}(n\alpha)]. \end{aligned}$$

Hemos así probado:

PROPOSICIÓN VI.2 (Fórmulas de De Moivre). *Si* $z = |z|(\cos\alpha + i\ \mathrm{sen}\,\alpha)$ *y* $n \in \mathbb{Z}$, *entonces:*

$$z^n = |z|^n[\cos(n\alpha) + i\ \mathrm{sen}(n\alpha)]. \qquad \square$$

La fórmula anterior nos dice que, en forma polar, es muy fácil calcular potencias de complejos. Veremos a continuación que calcular raíces de complejos también es sencillo. La situación es la siguiente: dado un número complejo $z = a + bi$ y un entero $n > 1$ queremos encontrar otro número complejo w tal que $w^n = z$, *i.e.*, $w = \sqrt[n]{z}$. Una primera pregunta que se ocurre

es: ¿cuántos complejos w existen que sean raíces n-ésimas de z? Aquí observamos que si $z = 0$ claramente la única raíz n-ésima es $w = 0$. Supongamos entonces que $z \neq 0$ y escribámoslo en forma polar $z = |z|(\cos\alpha + i\ \mathrm{sen}\,\alpha)$. Como el complejo w que buscamos debe satisfacer que $w^n = z$, entonces w debe ser $\neq 0$ también y por lo tanto lo podemos escribir en forma polar: $w = |w|(\cos\theta + i\ \mathrm{sen}\,\theta)$ de tal forma que para encontrar a w debemos hallar su módulo $|w|$ y su argumento θ (y es de esperarse que éstos aparezcan en términos del módulo y argumento de z y del entero n dado). Los detalles son como sigue: como $w^n = z$, usando la forma polar de w y z, y las fórmulas de De Moivre, obtenemos:

$$(*) \qquad |w|^n[\cos(n\theta) + i\ \mathrm{sen}(n\theta)] = |z|(\cos\alpha + i\ \mathrm{sen}\,\alpha)$$

y la igualdad de estos dos complejos implica que sus módulos son iguales, *i.e.*, $|w|^n = |z|$, por lo que

$$(1) \qquad |w| = \sqrt[n]{|z|},$$

(un número real positivo). También, la igualdad $(*)$ implica que los argumentos correspondientes deben ser iguales salvo un múltiplo entero de 2π, *i.e.*, $n\theta = \alpha + 2k\pi$ con $k \in \mathbb{Z}$. Se sigue que:

$$(2) \qquad \theta = \frac{\alpha + 2k\pi}{n} \quad \text{con } k \in \mathbb{Z}.$$

Las igualdades (1) y (2) definen complejos w cuya potencia n-ésima es z, *i.e.*. son raíces n-ésimas de z y como hemos visto se tiene un tal w para cada valor del argumento ya que el módulo es único. Para determinar cuántas raíces diferentes hay procedemos como sigue:

PRIMERO. Dado un entero $k \in \mathbb{Z}$, dividiéndolo entre n obtenemos $k = nq + r$ con $q, r \in \mathbb{Z}$ y $0 \leq r < n$. Observamos entonces que;

$$\theta = \frac{\alpha + 2k\pi}{n} = \frac{\alpha + 2(nq + r)\pi}{n} = \frac{\alpha + 2r\pi}{n} + 2q\pi,$$

i.e., el argumento correspondiente a $\dfrac{\alpha + 2k\pi}{n}$ es el mismo que el de $\dfrac{\alpha + 2r\pi}{n}$ ya que éstos difieren por el múltiplo $2q\pi$ de 2π. Por lo tanto, podemos restringir a $k \in \mathbb{Z}$ al rango $0 \leq k < n$, *i.e.*, $k = 0, 1, 2, \ldots, n-1$.

SEGUNDO. Dados dos enteros $j \neq k$ entre 0 y $n-1$, mostraremos que los argumentos $\dfrac{\alpha+2j\pi}{n}$ y $\dfrac{\alpha+2k\pi}{n}$ dan lugar a complejos diferentes (*i.e.*, no son iguales salvo un múltiplo entero de 2π). En efecto, si sucediera que

$$\frac{\alpha+2j\pi}{n} = \frac{\alpha+2k\pi}{n} + 2t\pi$$

entonces $\dfrac{\alpha+2j\pi}{n} = \dfrac{\alpha+2k\pi+2tn\pi}{n}$, por lo que $\alpha+2j\pi = \alpha+2k\pi+2tn\pi$, de donde cancelando α y luego dividiendo entre 2π obtenemos que $j = tn+k$, *i.e.*, $j-k = tn$, *i.e.*, $n|j-k$. Pero como $0 \leq j,k \leq n-1$, entonces la única posibilidad para que $n|j-k$ es que $j-k=0$ y por lo tanto $j=k$.

Hemos así probado:

PROPOSICIÓN VI.3. *Dado un complejo $z \neq 0$ en forma polar $z = |z|(\cos\alpha + i\,\mathrm{sen}\,\alpha)$. entonces z tiene exactamente n raíces complejas $w_k = |w_k|(\cos\theta_k + i\,\mathrm{sen}\,\theta_k)$ cuyos módulos son todos iguales:*

$$|w_k| = \sqrt[n]{|z|}$$

y cuyos argumentos son:

$$\theta_k = \frac{\alpha+2k\pi}{n} \quad \text{con } 0 \leq k \leq n-1. \qquad \square$$

Ejemplo 4. Calcule las raíces cúbicas de $z=1$.

En este ejemplo $|z|=1$, su argumento es $\alpha=0$ y $n=3$. Si $w = |w|[\cos\theta + i\,\mathrm{sen}\,\theta]$ es una de las 3 raíces cúbicas de z, entonces:

$$|w| = \sqrt[3]{|z|} = \sqrt[3]{1} = 1$$

y sus argumentos son

$$\theta_k = \frac{0+2k\pi}{3} = \frac{2k\pi}{3} \quad \text{para } k = 0,1,2,$$

por lo que:

Para $k=0$: $\theta_0 = \dfrac{0}{3} = 0.$

Para $k=1$: $\theta_1 = \dfrac{2\pi}{3}.$

Para $k = 2$: $\theta_2 = \dfrac{4\pi}{3} = 0$.

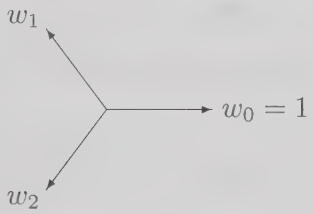
Así, las raíces cúbicas de $z = 1$ son:

$$w_0 = 1[\cos 0 + i \text{ sen } 0] = 1$$

$$w_1 = 1[\cos \frac{2\pi}{3} + i \text{ sen } \frac{2\pi}{3}] = \frac{1}{2} + \frac{\sqrt{3}}{2} i$$

$$w_2 = 1[\cos \frac{4\pi}{3} + i \text{ sen } \frac{4\pi}{3}] = -\frac{1}{2} - \frac{\sqrt{3}}{2} i.$$

Si graficamos estas tres raíces en el plano complejo obtenemos:



y observamos que las tres raíces cúbicas de $z = 1$ forman un triángulo equilátero. El ejercicio siguiente nos dice que esto sucede en el caso general:

EJERCICIO 17. Muestre que las n raíces n-ésimas de 1 son los vértices de un n-ágono regular inscrito en el círculo unitario, uno de cuyos vértices es 1.

EJERCICIO 18.

a) Calcule las raíces cuadradas de $w = i$.

b) Calcule las raíces cuartas de $w = -1 + \sqrt{3}\, i$.

c) Calcule las raíces sextas de $w = 1$.

d) Calcule las raíces cúbicas de $w = 8$.

e) Calcule las raíces cúbicas de $w = 1 - i$.

f) Calcule las raíces cuartas de $w = -16$.

g) Calcule las raíces quintas de $w = 32i$.

EJERCICIO 19. Demuestre que las raíces n-ésimas de $z = 1$ (diferentes de 1) satisfacen la ecuación *ciclotómica*:

$$u^{n-1} + u^{n-2} + \cdots + u + 1 = 0.$$

EJERCICIO 20. Considere el n-ágono regular inscrito en el círculo unitario en $\mathbb{C}$ y considere las $n-1$ diagonales obtenidas conectando un vértice fijo con todos los otros vértices. Demuestre que el producto de sus longitudes es n. *Sugerencia*: suponga que los vértices están unidos al vértice fijo 1 y aplique el ejercicio anterior.

EJERCICIO 21. Sea $n \geq 2$ un entero y considere el subconjunto $\mu_n \subseteq \mathbb{C}$ definido por:

$$\mu_n := \{u \in \mathbb{C} \ : \ u^n = 1\}.$$

a) Demuestre que μ_n es cerrado bajo productos, es decir, demuestre que si $u, v \in \mu_n$ entonces $uv \in \mu_n$.

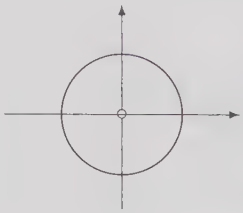
b) Demuestre que μ_n es cerrado bajo inversos, es decir, demuestre que si $u \in \mu_n$ entonces $u^{-1} \in \mu_n$.

c) La gráfica de μ_n en el plano complejo $\mathbb{C}$ está dada en el ejercicio 17.

Ejemplo 5. Si $r > 0$ es un número real, entonces el conjunto

$$\mathcal{C} := \{z \in \mathbb{C} \ : \ |z| = r\} \subseteq \mathbb{C}$$

es la circunferencia de centro el origen y radio r:

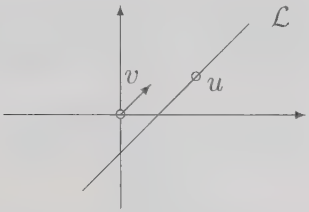


En general, si $c \in \mathbb{C}$ está fijo y $r > 0$ es un real, el conjunto

$$\mathcal{C} := \{z \in \mathbb{C} \ : \ |z - c| = r\} \subseteq \mathbb{C}$$

es la circunferencia de centro c y radio r.

Ejemplo 6. Sean $u, v \in \mathbb{C}$ complejos dados, con $v \neq 0$. Pensando a $u = (a, b)$ como un punto en el plano $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, y a $v \neq 0$ como un segmento dirigido, podemos considerar a la recta $\mathcal{L}$ que pasa por el punto u y es paralela al segmento dirigido v:



Como de $v \neq 0$ sólo nos interesa su dirección, podemos suponer que $|v| = 1$. ¿Cómo describir a la recta $\mathcal{L}$ en términos de los conceptos que tenemos de números complejos? Para hacer esto, observemos que un punto $z \in \mathbb{C}$ está en $\mathcal{L}$ si y sólo si existe $t \in \mathbb{R}$ tal que $z = u + tv$ (por la interpretación geométrica de la suma y producto de complejos). Así,

$$\mathcal{L} = \{z \in \mathbb{C} \,:\, z = u + tv, \ \text{ con } \ t \in \mathbb{R}\}.$$

Observamos ahora que, como $v \neq 0$,

$$z \in \mathcal{L} \ \Leftrightarrow \ z = u + tv \text{ con } \ t \in \mathbb{R} \ \Leftrightarrow \ \frac{z-u}{v} = t \in \mathbb{R} \ \Leftrightarrow \ \operatorname{Im}\left(\frac{z-u}{v}\right) = 0,$$

por lo que la recta $\mathcal{L}$ que pasa por el punto $u \in \mathbb{C}$ en la dirección $v \neq 0$, es el subconjunto del plano complejo dado por

$$\mathcal{L} = \{z \in \mathbb{C} \,:\, \operatorname{Im}\left(\frac{z-u}{v}\right) = 0\}.$$

Ejemplo 7. Sean $u, v \in \mathbb{C}$ dados, con $|v| = 1$. Queremos ahora describir el conjunto

$$\mathcal{H}_u := \{z \in \mathbb{C} \,:\, \operatorname{Im}\left(\frac{z-u}{v}\right) > 0\}.$$

(•) Comencemos con el caso cuando $u = 0$, de tal forma que el conjunto que tenemos ahora es

$$\mathcal{H}_0 := \{z \in \mathbb{C} \,:\, \operatorname{Im}(z/v) > 0\}.$$

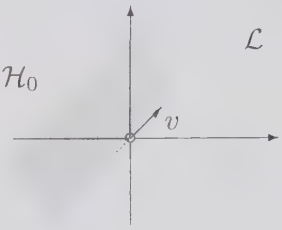
Escribiendo $v = \cos\phi + i \operatorname{sen}\phi$ (recordando que $|v| = 1$) y $z = r(\cos\theta + i \operatorname{sen}\theta)$ (con $r = |z|$), tenemos que

$$(z/v) = r[\cos(\theta - \phi) + i \operatorname{sen}(\theta - \phi)],$$

por lo que

$$z \in \mathcal{H}_0 \ \Leftrightarrow \ \operatorname{Im}(z/v) > 0 \ \Leftrightarrow \ \operatorname{sen}(\theta - \phi) > 0 \ \Leftrightarrow \ \phi < \theta < \pi + \phi,$$

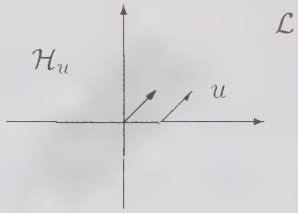
y por lo tanto $\mathcal{H}_0$ es el semiplano a la *izquierda* de la recta $\mathcal{L}$ que pasa por $u = 0$ paralela a v, si recorremos $\mathcal{L}$ en la dirección de v:



(•) Consideremos ahora el caso general

$$\mathcal{H}_u := \{z \in \mathbb{C} \ : \ \mathrm{Im}\left(\frac{z-u}{v}\right) > 0\}$$

y observemos que $\mathcal{H}_u = u + \mathcal{H}_0 = \{u + w \ : \ w \in \mathcal{H}_0\}$, es decir, $\mathcal{H}_u$ es $\mathcal{H}_0$ trasladado por u:



EJERCICIO 22. Describa los siguientes subconjuntos de $\mathbb{C}$:

a) $\{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0\}$.

b) $\{z \in \mathbb{C} \ : \ \mathrm{Re}(z) > 3/2\}$.

c) $\{z \in \mathbb{C} \ : \ |z-1| \leq 2\}$.

d) $\{z \in \mathbb{C} \ : \ |z+1| > 2\}$.

e) $\{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0, \frac{-1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}\}$.

f) $\{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0, \frac{-1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}, |z| \geq 1\}$.

EJERCICIO 23. Dados $u, v \in \mathbb{C}$, con $|v| = 1$, describa el siguiente subconjunto de $\mathbb{C}$:

$$\mathcal{J}_u := \{z \in \mathbb{C} \ : \ \mathrm{Im}\left(\frac{z-u}{v}\right) < 0\}.$$

VII. POLINOMIOS

Si K es un campo, por ejemplo $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{Z}/p\mathbb{Z}$ con p primo, un *polinomio con coeficientes en* K es una expresión de la forma

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

con $a_j \in K$ y $n \geq 0$ un entero. Denotaremos al conjunto de polinomios con coeficientes en K con $K[x]$.

Dos polinomios $f(x) = a_0 + a_1 + \cdots + a_m x^m$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ en $K[x]$, son iguales, denotado $f(x) = g(x)$, si y sólo si $a_j = b_j$ en K para todo $j \geq 0$. En particular, $m = n$. Así, un polinomio está determinado por sus coeficientes. Los polinomios de la forma $f(x) = a_0$ con $a_0 \in K$ se llaman *polinomios constantes.*

En $K[x]$ se tienen la *suma* y *producto* usuales:

- Suma. Si $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ y $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ son dos polinomios en $K[x]$, se define

  $$f(x) + g(x) := (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_i + b_i)x^i + \cdots,$$

  notando que cada $(a_i + b_i) \in K$ por lo que $f(x) + g(x) \in K[x]$.

- Producto. Si $f(x), g(x) \in K[x]$ son dos polinomios dados como antes, se define

  $$f(x) \cdot g(x) := a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + c_k x^k + \cdots,$$

  donde

  $$c_k := \sum_{i+j=k} a_i \cdot b_j.$$

Notamos que cada c_k es una suma de productos de elementos de K por lo que $c_k \in K$ y así $f(x)g(x) \in K[x]$.

Teorema VII.1. *El conjunto $K[x]$ con las operaciones anteriores es un anillo conmutativo con uno.*

Demostración. Sólo probaremos algunas de las propiedades de anillo de $K[x]$. El polinomio $0 \in K[x]$ es el que tiene todos sus coeficientes $a_j = 0$.

Si $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ su inverso aditivo es el polinomio $-f(x) := -a_0 - a_1x - a_2x^2 - \cdots - a_nx^n$, con los $-a_j \in K$. El uno de $K[x]$ es el polinomio constante $f(x) = 1$. □

EJERCICIO 1. Justifique las otras propiedades de anillo conmutativo de $K[x]$ en el teorema anterior.

El grado de un polinomio. Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ es un polinomio no cero en $K[x]$, se define su *grado* como

$$\operatorname{gr}\big(f(x)\big) := n \qquad \text{si} \qquad a_n \neq 0.$$

Al elemento a_n se le llama el *coeficiente de grado* del polinomio $f(x)$. Así, los polinomios constantes no cero $f(x) = a_0 \neq 0$, tienen grado $\operatorname{gr}(a_0) = 0$. Al polinomio 0 no se le asigna grado, o en ocasiones se le asigna el grado $-\infty$, donde el símbolo $-\infty$ satisface que $-\infty < n$ para todo $n \in \mathbb{N} \cup \{0\}$, y $-\infty + (-\infty) = -\infty$, $-\infty + n = -\infty$ y $-\infty \cdot n = -\infty$ si $n \neq 0$. Nosotros usaremos esta última convención. De esta definición se sigue inmediatamente,

LEMA VII.2. *Si $f(x), g(x)$ son polinomios en $K[x]$, entonces*

(1) $\operatorname{gr}(f \cdot g) = \operatorname{gr}(f) + \operatorname{gr}(g)$.

(2) $\operatorname{gr}(f + g) \leq \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}$.

Demostración. Escribamos $f(x) = a_0 + a_1x + \cdots + a_mx^m$ y $g(x) = b_0 + b_1x + \cdots + b_nx^n$.
(1) Si $f(x) = 0$ o $g(x) = 0$, entonces $f(x)g(x) = 0$ y si, por ejemplo, $f(x) = 0$, se tiene que

$$\operatorname{gr}(fg) = \operatorname{gr}(0) = -\infty = -\infty + \operatorname{gr}(g) = \operatorname{gr}(0) + \operatorname{gr}(g) = \operatorname{gr}(f) + \operatorname{gr}(g).$$

Supongamos entonces que $f(x) \neq 0$ y $g(x) \neq 0$, entonces $a_m \neq 0$ y $b_n \neq 0$ en K. En el producto $f(x)g(x) = c_0 + c_1x + \cdots + c_kx^k + \cdots$ se tiene que $c_k = \sum_{i+j=k} a_ib_j$. Mostraremos que

$$\operatorname{gr}(fg) = m + n = \operatorname{gr}(f) + \operatorname{gr}(g),$$

i.e., mostraremos que $c_{m+n} \neq 0$ y que $c_k = 0$ para toda $k > m + n$. En efecto,

(I) Si $k > m+n$ entonces en $c_k = \sum_{i+j=k} a_i b_j$ se tiene que $i+j > m+n$ y así no se puede tener que $i \leq m$ y $j \leq n$ por lo que $i > m$ o $j > n$. Si $i > m$ el coeficiente correspondiente $a_i = 0$ y así $a_i b_j = 0$ para todo j. Similarmente, si $j > n$ el coeficiente $b_j = 0$ por lo que $a_i b_j = 0$ para todo i. Se sigue que todos los sumandos en c_k con $k > m+n$ son 0 y por lo tanto $c_k = 0$ para toda $k > m+n$.

(II) Si $k = m+n$, entonces en $c_{m+n} = \sum_{i+j=m+n} a_i b_j$ los índices i, j satisfacen:

- Si $i < m$ como $i+j = m+n$ entonces $j > n$ y así $b_j = 0$ por lo que el sumando $a_i b_j = 0$.
- Si $j < n$ entonces $i > m$ y así $a_i = 0$ por lo que el sumando correspondiente $a_i b_j = 0$.
- La última posibilidad es que $i = m$ y $j = n$ y en este caso el sumando correspondiente es $a_m b_n$ el cual es $\neq 0$ ya que $a_m \neq 0$ y $b_n \neq 0$ en K que es un campo y por lo tanto un dominio entero.

Se sigue que $c_{m+n} = a_m b_n \neq 0$ y es el coeficiente de grado de $f(x)g(x)$, *i.e.*, $\operatorname{gr}(fg) = m+n = \operatorname{gr}(f) + \operatorname{gr}(g)$.

(2) Si $f(x) = 0$ o $g(x) = 0$, la desigualdad se verifica fácilmente. Supongamos entonces que $f(x) \neq 0$ y $g(x) \neq 0$. Entonces $a_m \neq 0$ y $b_n \neq 0$ y $\operatorname{gr}(f) = m$, $\operatorname{gr}(g) = n$. Supongamos que $m \geq n$. Consideremos la suma

$$f(x) + g(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_k x^k + \cdots$$

con $d_k = a_k + b_k$ donde estamos suponiendo que $m \geq n$.

Si sucediera que $m > n$ entonces el coeficiente $b_m = 0$ y por lo tanto $d_m = a_m + b_m = a_m + 0 = a_m \neq 0$ y así $\operatorname{gr}(f+g) = \operatorname{gr}(f) = m$.

Si sucediera que $m = n$, entonces $c_m = a_m + b_m$ y $c_k = 0$ para toda $k > m$, por lo que $\operatorname{gr}(f + g) \leq m$ (puede ser estrictamente menor si $a_m = -b_m$). □

Una consecuencia inmediata es:

COROLARIO VII.3. *El anillo $K[x]$ es un dominio entero.*

Demostración. En efecto, si $f(x), g(x) \in K[x] - \{0\}$, entonces $\text{gr}(f) \geq 0$ y $\text{gr}(g) \geq 0$,

$$gr(f \cdot g) = \text{gr}(f) + \text{gr}(g) \geq 0$$

y por lo tanto $f(x) \cdot g(x) \neq 0$. □

VII.1 Divisibilidad en anillos de polinomios

El dominio entero $K[x]$ es formalmente parecido al dominio entero $\mathbb{Z}$ y así como tenemos una teoría de divisibilidad en $\mathbb{Z}$, tenemos lo análogo para $K[x]$. Comenzamos con el algoritmo de la división donde el papel que desempeña el *valor absoluto* de un número entero, que nos permite dar un tamaño del entero, corresponde ahora al *grado* de un polinomio. Por ejemplo, de la parte (1) del lema (VII.2), se tiene que

(i) Si $f(x), g(x) \in K[x] - \{0\}$, entonces

$$\text{gr}(f) \leq \text{gr}(f \cdot g)$$

ya que $\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g) \geq \text{gr}(f)$.

(ii) Para el *algoritmo de la división*, que no es otra cosa que la división con residuo de polinomios, tenemos:

Proposición VII.4. *Sea K un campo y sean $f, g \in K[x]$, con $g \neq 0$. Entonces, existen polinomios únicos $q(x)$, $r(x) \in K[x]$ tales que*

$$f(x) = g(x) \cdot q(x) + r(x)$$

con $r(x) = 0$ o $\text{gr}(r) < \text{gr}(g)$.

Demostración. Primero, si $\text{gr}(f) < \text{gr}(g)$, entonces poniendo $q(x) = 0$ y $r(x) = f(x)$ se tiene el resultado deseado.

Supongamos entonces que $\text{gr}(f) = m \geq n = \text{gr}(g)$, y escribamos

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$
$$g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

con $b_n \neq 0$.

Para dividir $f(x)$ entre $g(x)$, el primer término del cociente es

$$\frac{a_m}{b_n}x^{m-n}$$

que luego se multiplica por $g(x)$ y el resultado se resta a $f(x)$ para obtener

$$f_1(x) := f(x) - \left(\frac{a_m}{b_n}\right)x^{m-n} \cdot g(x) \tag{1}$$

donde observamos que el término de mayor grado en $f(x)$, $a_m x^m$, se cancela con el término

$$-\left(\frac{a_m}{b_n}\right)x^{m-n} \cdot (b_n x^n) = -a_m x^m$$

y así,

$$\operatorname{gr}(f_1) < \operatorname{gr}(f).$$

Procedemos ahora por inducción sobre el grado n de $f(x)$. Por hipótesis de inducción se tiene que

$$f_1(x) = g(x)q_1(x) + r(x) \tag{2}$$

con $q_1(x), r(x) \in K[x]$ y $r(x) = 0$ o $\operatorname{gr}(r) < \operatorname{gr}(g)$.

Substituyendo (2) en (1),

$$f(x) - \left(\frac{a_m}{b_n}x^{m-n}g(x)\right) = g(x)q_1(x) + r(x)$$

y así,

$$f(x) = \left(\frac{a_m}{b_n} \cdot x^{m-n} + q_1(x)\right)g(x) + r(x)$$

con $q(x) := (a_m/b_n)x^{m-n} + q_1(x) \in K[x]$ y $r(x) = 0$ o $\operatorname{gr}(r) < \operatorname{gr}(g)$ como se quería probar.

Finalmente, para probar la *unicidad* de $q(x)$ y $r(x)$ con las propiedades requeridas, supongamos que $\tilde{q}(x)$ y $\tilde{r}(x)$ son otros polinomios en $K[x]$ tales que

$$f(x) = g(x)\tilde{q}(x) + \tilde{r}(x)$$

con $\tilde{r}(x) = 0$ o $\operatorname{gr}(\tilde{r}) < \operatorname{gr}(g)$. Entonces, de

$$f(x) = g(x)q(x) + r(x)$$

restando, se sigue

$$g(x) \cdot \big(q(x) - \tilde{q}(x)\big) = r(x) - \tilde{r}(x) \tag{3}$$

y en esta igualdad, como por hipótesis $g(x) \neq 0$, y $K[x]$ es un dominio entero, se sigue $r - \tilde{r} = 0 \Leftrightarrow q - \tilde{q} = 0$. Ahora, si $q - \tilde{q} \neq 0$, de la igualdad (3) y del lema (VII.2)(1), se sigue que

$$\mathrm{gr}(r - \tilde{r}) = \mathrm{gr}(g) + \mathrm{gr}(q - \tilde{q}) \geq \mathrm{gr}(g)$$

y del mismo lema (VII.2)(2) se tiene que

$$\mathrm{gr}(r - \tilde{r}) \leq \mathrm{máx}\{\mathrm{gr}(r), \mathrm{gr}(\tilde{r})\} < \mathrm{gr}(g),$$

una contradicción. Se sigue $r = \tilde{r}$ y $q = \tilde{q}$. □

Dados dos polinomios $f(x), g(x) \in K[x]$ con $g(x) \neq 0$, diremos que $g(x)$ *divide a* $f(x)$ en $K[x]$ si $f(x) = g(x)q(x)$ con $q(x) \in K[x]$, *i.e.*, si el residuo $r(x)$ de dividir $f(x)$ entre $g(x)$ es 0. Usaremos la misma notación que en $\mathbb{Z}$ y escribiremos $g(x)|f(x)$. Las propiedades siguientes se demuestran como en $\mathbb{Z}$:

EJERCICIO 2. Sean K un campo y $K[x]$ el anillo de polinomios con coeficientes en K. Demuestre que:

(1) $\forall\, f(x) \neq 0$ en $K[x]$ se tiene que $f(x)|f(x)$.

(2) $\forall\, \alpha \neq 0$ en K y $\forall\, f(x) \in K[x]$ se tiene que $\alpha|f(x)$.

(3) $\forall\, f(x) \neq 0$ en $K[x]$ se tiene que $f(x)|0$.

(4) Si $f(x)|g(x)$ y $g(x)|h(x)$, entonces $f(x)|h(x)$.

(5) Si $f(x)|g(x)$ y $f(x)|h(x)$, entonces $f(x)|g(x) + h(x)$.

(6) Si $f(x)|g(x)$ y $h(x) \in K[x]$ es arbitrario, entonces $f(x)|g(x)h(x)$.

(7) Se sigue que si $f(x)|g(x)$ y $f(x)|h(x)$, entonces para todos los

$$s(x), t(x) \in K[x]$$

se tiene que $f(x)$ divide a la combinación lineal:

$$f(x)|g(x)s(x) + h(x)t(x).$$

(8) $f(x)|1 \Leftrightarrow f(x) = \alpha \neq 0$ con $\alpha \in K$.

(9) Los elementos de $K[x]$ que tienen inverso multiplicativo son los polinomios constantes $\neq 0$.

(10) Si $f(x)|g(x)$ y $g(x)|f(x)$, entonces existe una constante $\alpha \neq 0$ en K tal que $f(x) = \alpha g(x)$. (En este caso diremos que $f(x)$ y $g(x)$ son *asociados.*)

El máximo común divisor. Dados dos polinomios $f(x), g(x) \in K[x]$, un *máximo común divisor* de $f(x)$ y $g(x)$ es un polinomio $d(x) \in K[x]$ tal que:

(I) $d(x)|f(x)$ y $d(x)|g(x)$.

(II) Si $h(x)|f(x)$ y $h(x)|g(x)$, entonces $h(x)|d(x)$.

EJERCICIO 3. Sean $f(x), g(x) \in K[x] - \{0\}$ y sean $d_1(x)$ y $d_2(x)$ máximos comunes divisores de $f(x)$ y $g(x)$. Demuestre que d_1 y d_2 son asociados. Denotaremos por $\text{mcd}(f(x), g(x))$ a un mcd de f y g.

TEOREMA VII.5. *Si $f(x), g(x) \in K[x]$, con alguno de ellos $\neq 0$, entonces existe un* $\text{mcd}(f, g)$ *y, de hecho, es la combinación lineal de menor grado ≥ 0 de $f(x)$ y $g(x)$.*

Demostración. Sea

$$M = \{\text{gr}(f(x)s(x) + g(x)t(x)) \ : \ f(x)s(x) + g(x)t(x) \neq 0\} \subseteq \mathbb{N} \cup \{0\}$$

y notemos que $M \neq \emptyset$ poniendo $s = 1$ y $t = 0$ si $f \neq 0$ o $s = 0$ y $t = 1$ si $g \neq 0$. Por el principio del buen orden existe un $d(x) = f(x)s(x) + g(x)t(x) \neq 0$ de grado menor en M.

Mostraremos ahora que $d|f$ y $d|g$. Es claro que, por simetría, basta mostrar que $d|f$. Para esto, supongamos que $d \nmid f$; entonces $f = dq + r$ con $r \neq 0$ y $0 \leq \text{gr}(r) < \text{gr}(d)$. Se sigue que

$$r = f - dq = f - (fs + gt)q = f(1 - sq) + g(-tq) \in M$$

con $\text{gr}(r) < \text{gr}(d)$, en contradicción con la minimalidad del grado de d. Se sigue que $d|f$ y similarmente $d|g$.

Supongamos ahora que $h(x) \in K[x]$ es tal que $h|f$ y $h|g$. Se sigue que h divide a cualquier combinación lineal de f y g, en particular $h|d$.

Hemos mostrado así que d satisface las propiedades de mcd de f y g, *i.e.*, $d = \text{mcd}(f, g)$. □

EJERCICIO 4. Formule y demuestre el *algoritmo de Euclides* en $K[x]$ para hallar el mcd de dos polinomios $f(x), g(x) \in K[x]$. *Sugerencia*: vea el algoritmo de Euclides en $\mathbb{Z}$.

EJERCICIO 5. Usando el algoritmo anterior calcule el mcd de los polinomios $f(x) = x^3 + 3x^2 + 3x + 1$ y $g(x) = x^4 + 2x^3 - x^2 - 4x - 2$.

Diremos que dos polinomios $f(x), g(x) \in K[x]$ son *coprimos* si su mcd es (asociado a) 1, *i.e.*, si su mcd es un elemento invertible en $K[x]$.

EJERCICIO 6. Demuestre que si $f(x)|g(x)h(x)$ en $K[x]$ y $\text{mcd}(f, g) = 1$ entonces $f|h$.

Primos o irreducibles en $K[x]$. En completa analogía con el caso de $\mathbb{Z}$, podemos ahora considerar polinomios primos en $K[x]$: un polinomio $p(x) \in K[x]$ se dice que es *primo* o *irreducible* si no es constante y sus únicos divisores son elementos invertibles (*i.e.*, constantes $\alpha \neq 0$ en K) o asociados de $p(x)$ (*i.e.*, polinomios de la forma $\alpha p(x)$ con $\alpha \in K - \{0\}$).

Ejemplo 1. Si K es cualquier campo, en el anillo $K[x]$ los polinomios de primer grado $ax + b \in K[x]$, $a \neq 0$, son irreducibles. Nótese que como $a \neq 0$ podemos escribir $ax + b = a(x + \frac{b}{a})$ con $b/a \in K$, por lo que el polinomio $ax + b$ es asociado de un polinomio primo de la forma $x + \alpha$ con $\alpha \in K$.

EJERCICIO 7. Si $p(x) \in K[x]$ es un polinomio irreducible y $p(x)|f(x)g(x)$ en $K[x]$, demuestre que $p(x)|f(x)$ o $p(x)|g(x)$.

El resultado principal es:

TEOREMA VII.6 (Factorización única). *Si K es un campo entonces todo polinomio no constante $f(x) \in K[x]$ se puede factorizar de la forma*

$$f(x) = p_1(x) \cdots p_r(x)$$

con los $p_j(x) \in K[x]$ irreducibles. Más aún, si

$$f(x) = q_1(x) \cdots q_s(x)$$

es otra factorización de $f(x)$ con los $q_j(x)$ irreducibles en $K[x]$, entonces $r = s$ y $p_i(x) = u_{j(i)}q_{j(i)}(x)$ para alguna permutación de los índices y donde $u_{j(i)}$ es una constante $\neq 0$. Dicho en otras palabras, la factorización es única salvo el orden de los factores y asociados.

Demostración. La demostración es completamente análoga a la del teorema fundamental de la aritmética (III.21), sólo que ahora el papel del *valor absoluto* de un entero lo desempeña el concepto de *grado* de un polinomio.

Existencia de la factorización. Por inducción sobre el grado de $f(x) \in K[x]$, el cual es ≥ 1 ya que $f(x)$ no es constante. Primero, si $f(x) = p(x)$ es irreducible, entonces esta igualdad es la factorización deseada. Si $f(x)$ es compuesto, entonces lo podemos escribir como $f(x) = g(x)h(x)$ con g, h polinomios tales que $1 \leq \mathrm{gr}(g), \mathrm{gr}(h) < \mathrm{gr}(f)$. Por hipótesis de inducción g y h se pueden factorizar en producto de primos:

$$g(x) = p_1(x) \cdots p_r(x) \quad \text{y} \quad h(x) = q_1(x) \cdots q_s(x),$$

con los $p_i(x)$ y $q_j(x)$ primos de $K[x]$. Se sigue que

$$f(x) = p_1(x) \cdots p_r(x) q_1(x) \cdots q_s(x)$$

es la factorización deseada de $f(x)$.

Unicidad de la factorización. Supongamos que

$$f(x) = p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x)$$

son dos factorizaciones de $f(x)$ con los $p_i(x)$ y $q_j(x)$ primos. Sin perder generalidad podemos suponer que $r \leq s$. Ahora, de la igualdad

$$p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x)$$

se sigue que $p_1 | q_1 \cdots q_s$ y como p_1 es primo, por el ejercicio 7 esto implica que p_1 divide a algún q_j. Ahora, reordenando si hiciera falta podemos suponer que $q_j = q_1$ por lo que $p_1 | q_1$ con ambos primos; se sigue que $q_1 = u_1 p_1$ con $u_1 \in K - \{0\}$ una unidad. Así, de la igualdad

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

con $q_1 = u_1 p_1$ y como $K[x]$ es un dominio entero, podemos cancelar el factor p_1 en la igualdad anterior para obtener:

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

De nuevo, esto implica que p_2 divide a $q_2 \cdots q_s$ por lo que p_2 divide algún q_j para $2 \leq j \leq s$, y reordenando si hiciera falta podemos suponer que $q_j = q_2$; como p_2 y q_2 son primos, entonces $q_2 = u_2 p_2$ con u_2 una unidad y procedemos como antes para cancelar a p_2, etcétera. Como $r < s$, al cancelar todos los p_i queda:

$$1 = u q_{r+1} \cdots q_s$$

(con $u \in K - \{0\}$) lo cual es imposible a menos que $r = s$ y que $p_i = q_i$ (salvo una constante no cero) después de los reordenamientos adecuados. □

Usando este teorema, dado un polinomio no constante $f(x)$ en $K[x]$ y su factorización $f(x) = p_1(x) \cdots p_r(x)$ en factores irreducibles, reuniendo los factores primos iguales podemos escribir esta factorización como:

$$f(x) = p_1(x)^{m_1} \cdots p_s(x)^{m_s}$$

con los $m_j \geq 1$.

VII.2 Raíces o ceros de un polinomio

Antes de dar más ejemplos de polinomios irreducibles es conveniente formalizar la noción de *raíz* o *cero* de un polinomio $f(x) \in K[x]$. Escribamos

$$f(x) = a_0 + a_1 x + \cdots a_n x^n.$$

Para cada $\alpha \in K$ se define

$$f(\alpha) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n \in K.$$

Un elemento $\alpha \in K$ se llama un *cero* o *raíz* del polinomio $f(x)$ si $f(\alpha) = 0$.

Lema VII.7. *Sea K un campo y sea $\alpha \in K$. La función $K[x] \to K$, llamada evaluación en α, dada por $f(x) \mapsto f(\alpha)$, preserva las operaciones de $K[x]$ y K.*

Demostración. Sean

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$

y

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

polinomios en $K[x]$. Como

$$(f+g)(x) = (a_0+b_0) + (a_1+b_1)x + \cdots + (a_j+b_j)x^j + \cdots,$$

entonces,

$$\begin{aligned}(f+g)(\alpha) &= (a_0+b_0) + (a_1+b_1)\alpha + \cdots + (a_j+b_j)\alpha^j + \cdots \\ &= (a_0 + a_1\alpha + a_2\alpha^2 + \cdots) + (b_0 + b_1\alpha + b_2\alpha^2 + \cdots) \\ &= f(\alpha) + g(\alpha).\end{aligned}$$

Similarmente,

$$(fg)(\alpha) = f(\alpha)g(\alpha). \qquad \square$$

EJERCICIO 8. Sean K un campo y $\alpha \in K$. Demuestre que la función evaluación en α del lema anterior $ev_\alpha : K[x] \to K$ es suprayectiva pero no es inyectiva.

Nuestro siguiente objetivo es relacionar la noción de raíz de un polinomio con la factorización de éste:

TEOREMA VII.8 (Teorema del residuo). *Sean K un campo y $f(x) \in K[x]$ un polinomio. Entonces, para todo $\alpha \in K$, el residuo de dividir $f(x)$ entre $x - \alpha \in k[x]$ es $f(\alpha)$.*

Demostración. Dividiendo $f(x) \in K[x]$ entre $x - \alpha \in K[x]$, se obtiene

$$(*) \qquad f(x) = (x-\alpha)q(x) + r(x)$$

donde $r(x) = 0$ o $\mathrm{gr}(r) < \mathrm{gr}(x-\alpha) = 1$. En cualquier caso, $r(x)$ es un polinomio constante, digamos $r(x) = r \in K$. Evaluando $(*)$ en $x = \alpha$ y usando el lema anterior, se tiene que

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r,$$

como se quería demostrar. $\square$

COROLARIO VII.9. *Sea K un campo y sea $f(x) \in K[x]$ un polinomio. Entonces, $\alpha \in K$ es un cero de $f(x)$ si y sólo si $x - \alpha | f(x)$ en $K[x]$.*

Demostración. Si $\alpha \in K$ es cero de $f(x)$, el residuo r de dividir $f(x)$ entre $x - \alpha$ es $0 = f(\alpha)$ por el teorema anterior, y así $x - \alpha | f(x)$.

Si $x - \alpha | f(x)$, entonces $f(x) = (x - \alpha)q(x)$, y evaluando en $x = \alpha$ se tiene que $f(\alpha) = (\alpha - \alpha)q(\alpha) = 0$. □

EJERCICIO 9. Si $f(x) \in K[x]$ y $\alpha \in K$, demuestre que $x - \alpha | f(x) - f(\alpha)$.

EJERCICIO 10. Si $f(x) | g(x)$ en $K[x]$, demuestre que toda raíz de $f(x)$ es raíz de $g(x)$.

Dado un polinomio $f(x) \in K[x]$, si $\alpha \in K$ es una raíz de $f(x)$, entonces el corolario anterior nos dice que

$$f(x) = (x - \alpha)q_1(x) \tag{1}$$

con $q_1(x) \in K[x]$. Pudiera suceder entonces que α también fuera raíz de $q_1(x)$, en cuyo caso también tendríamos que

$$q_1(x) = (x - \alpha)q_2(x)$$

con $q_2(x) \in K[x]$, y así substituyendo en (1) se tendría que

$$f(x) = (x - \alpha)^2 q_2(x). \tag{2}$$

Podemos continuar este proceso si α es raíz de $q_2(x)$, hasta obtener

$$f(x) = (x - \alpha)^m q_m(x) \tag{3}$$

con $q_m(x) \in K[x]$, $m \geq 1$. Nótese que el proceso anterior debe terminar, *i.e.*, existe un entero $m \geq 1$ tal que $q_m(\alpha) \neq 0$, ya que

$$\text{gr}(f) = \text{gr}(x - \alpha)^m + \text{gr}(q_m) = m + \text{gr}(q_m),$$

y así tanto m como $\text{gr}(q_m)$ son $\leq \text{gr}(f)$.

Multiplicidad. Sea K un campo y sea $f(x) \in K[x]$ un polinomio. Un elemento $\alpha \in K$ se llama un *cero de multiplicidad* $m \geq 1$ de $f(x)$ si $(x - \alpha)^m | f(x)$ pero $(x - \alpha)^{m+1} \nmid f(x)$.

Si $m = 1$, diremos que α es una raíz *simple*. Si $m > 1$, diremos que α es una raíz *múltiple*.

Con este concepto a la mano ya podemos considerar la pregunta de cómo contar las raíces de un polinomio $f(x) \in K[x]$: cada raíz α de $f(x)$ se debe contar con su multiplicidad, *i.e.*, si α es una raíz de multiplicidad m, entonces la contamos m veces. Con la convención de contar las raíces de un polinomio teniendo en cuenta su multiplicidad, podemos preguntarnos ahora: dado un polinomio no cero $f(x) \in K[x]$, ¿cuántas raíces puede tener $f(x)$ en K?

TEOREMA VII.10. *Sea $f(x) \in K[x]$ un polinomio de grado $n \geq 1$. Entonces, el número de raíces de $f(x)$ en K, contadas con su multiplicidad, es menor o igual que n.*

Más aún, si $\alpha_1, \ldots, \alpha_r \in K$ son todas las raíces de $f(x)$ en K, con multiplicidades $m_1, \ldots, m_r$ respectivamente, entonces

$$f(x) = (x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r} g(x),$$

donde $g(x) \in K[x]$ no tiene raíces en K.

Demostración. Primero mostraremos que el número de raíces de $f(x)$ en K es $\leq n$. La demostración es por inducción sobre $n \geq 1$.

(1) Si $n = 1$, entonces $f(x) = a_0 + a_1 x \in K[x]$, con $a_1 \neq 0$. Entonces, para cualquier $\alpha \in K$ tal que

$$0 = f(\alpha) = a_0 + a_1 \alpha$$

se debe tener que $\alpha = -a_0/a_1$, y así α está unívocamente determinada por los coeficientes de $f(x)$.

(2) Supongamos ahora que el resultado es verdadero para todos los polinomios de grado menor que n, y sea $f(x) \in K[x]$ un polinomio de grado $n > 1$:

(I) Si $f(x)$ no tiene raíces en K, entonces el teorema es cierto ya que $0 < n$.

(II) Si $f(x) \in K[x]$ tiene al menos una raíz $\alpha \in K$ de multiplicidad $m \geq 1$, entonces en $K[x]$ se tiene que

$$f(x) = (x - \alpha)^m g(x)$$

con $g(x) \in K[x]$ y $g(\alpha) \neq 0$.

Como $(x-\alpha)^m | f(x)$, entonces $m \leq \text{gr}(f) = n$, y de hecho

$$n = \text{gr}(f) = \text{gr}(x-\alpha)^m + \text{gr}(g) = m + \text{gr}(g),$$

y así $\text{gr}(g) = n - m \geq 0$.

Observemos ahora que cualquier raíz β de $f(x)$ con $\beta \neq \alpha$, debe ser una raíz de $g(x)$ ya que

$$0 = f(\beta) = (\beta - \alpha)^m g(\beta)$$

y como $\beta - \alpha \neq 0$, entonces $g(\beta) = 0$.

Ahora, si $m = n$, como $\text{gr}(g) = n - m = 0$, entonces g debe ser un polinomio constante no cero en $K[x]$, y por lo tanto no tiene raíces. Se sigue que $f(x)$ tiene una única raíz $\alpha \in K$ de multiplicidad $m = n \leq n$.

Ahora, si $m < n$, como $\text{gr}(g) = n - m < n = \text{gr}(f)$, entonces por hipótesis de inducción $g(x) \in K[x]$ tiene a lo más $n - m$ raíces en K, y como, por la observación de arriba, todas las raíces de $f(x)$ diferentes de α deben ser raíces de $g(x)$, entonces $f(x)$ tiene a lo más $m + (n - m) = n$ raíces en K, como se quería demostrar.

Finalmente, si $\alpha_1, \ldots, \alpha_r \in K$ son todas las raíces de $f(x)$ en K con multiplicidades $m_1, \ldots, m_r$ respectivamente, entonces por lo demostrado arriba, $r \leq n = \text{gr}(f)$ y de hecho $m_1 + \cdots + m_r \leq n$. También, como α_1 es raíz de $f(x)$ de multiplicidad m_1, entonces

$$f(x) = (x - \alpha_1)^{m_1} g_1(x)$$

con $g_1(\alpha_1) \neq 0$.

Ahora, si $\alpha_2 \neq \alpha_1$ es otra raíz de $f(x)$, con multiplicidad m_2, entonces como observamos arriba, α_2 debe ser raíz de $g_1(x)$, y así

$$g_1(x) = (x - \alpha_2)^{m_2} g_2(x)$$

con $g_2(\alpha_2) \neq 0$ y también $g_2(\alpha_1) \neq 0$. Se sigue que

$$f(x) = (x - \alpha_1)^{m_1} (x - \alpha_2)^{m_2} g_2(x)$$

con $g_2(\alpha_1) \neq 0$ y $g_2(\alpha_2) \neq 0$.

Inductivamente se obtiene

$$f(x) = (x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r} g_r(x)$$

con $g_r(x) \in K[x]$ y $g_r(\alpha_j) \neq 0$ para toda $j = 1, \ldots, r$. Más aún, $g_r(x)$ no tiene ya raíces en K ya que de lo contrario $f(x)$ tendría otra raíz en K diferente de las α_j, en contradicción con la hipótesis. □

VII.2.1 Derivadas de polinomios y multiplicidad de raíces

Para determinar si un polinomio $f(x) \in K[x]$ tiene raíces múltiples se tiene un criterio sencillo que involucra a la derivada del polinomio; sin embargo, como los coeficientes de $f(x)$ están en un campo arbitrario, el concepto de derivada de un polinomio es completamente formal (¡nada de límites!). La definición siguiente es lo que podríamos esperar:

Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, su *derivada* es el polinomio

$$f'(x) := a_1 + 2a_2x + \cdots + na_nx^{n-1} \in K[x].$$

Las propiedades siguientes son inmediatas de esta definición:

EJERCICIO 11. Sea K un campo y sean f, $g \in K[x]$. Demuestre que:

(1) $(f+g)' = f' + g'$

(2) $(f \cdot g)' = f \cdot g' + f' \cdot g$.

Y para el polinomio constante $f = a \in K$, se tiene que

(3) $(a)' = 0$, y consecuentemente

(4) $(a \cdot f)' = a \cdot f'$, para toda $a \in K$.

El lema siguiente nos da un criterio para decidir cuándo un polinomio dado tiene raíces múltiples:

LEMA VII.11. *Sean K un campo, $f(x) \in K[x]$ un polinomio no cero y $\alpha \in K$ una raíz de $f(x)$. Entonces, α es una raíz múltiple de $f(x)$ si y sólo si α es raíz de f y f'.*

Demostración. Si $\alpha \in K$ es un cero de multiplicidad $m \geq 2$ de $f(x)$, entonces en $K[x]$,

$$f(x) = (x-\alpha)^m g(x), \qquad \text{con } m \geq 2,$$

y así, usando el ejercicio anterior,

$$\begin{aligned} f'(x) &= m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x) \\ &= (x-\alpha)^{m-1}[m\, g(x) + (x-\alpha)g'(x)] \end{aligned}$$

con $m - 1 \geq 1$, por lo que $f(x)$ y $f'(x)$ tienen el factor común $(x-\alpha)^{m-1}$ de grado ≥ 1, en particular α es raíz de $f'(x)$.

Supongamos que $\alpha \in K$ es raíz de $f(x)$ y de $f'(x)$ y sea $m \geq 1$ la multiplicidad de α como raíz de $f(x)$. Mostraremos que $m \geq 2$, *i.e.*, mostraremos que si

$$(*) \qquad f(x) = (x - \alpha)g(x)$$

entonces $(x - \alpha)|g(x)$ en $K[x]$.

En efecto, derivando la igualdad $(*)$ obtenemos:

$$(\dagger) \qquad f'(x) = (x - \alpha)g'(x) + g(x)$$

donde $(x - \alpha)$ divide a $f'(x)$ por hipótesis y claramente también divide a $(x - \alpha)g'(x)$; se sigue que $(x - \alpha)|g(x)$, como se quería. □

EJERCICIO 12. Determine la multiplicidad de la raíz $\alpha = 1$ en cada uno de los polinomios siguientes con coeficientes en $\mathbb{Q}$:

(1) $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$.

(2) $g(x) = x^4 - x^3$.

(3) $h(x) = x^5 - 3x^4 + 5x^3 - 4x^2 + 3x - 2$.

EJERCICIO 13. Si $K = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ y $f(x) \in K[x]$, demuestre que $\alpha \in K$ es una raíz de $f(x)$ de multiplicidad m si y sólo si

$$0 = f(\alpha) = f'(\alpha) = f''(\alpha) = \cdots = f^{(m-1)}(\alpha)$$

y

$$f^{(m)}(\alpha) \neq 0.$$

VII.3 EXPANSIÓN DE TAYLOR DE UN POLINOMIO

Si $f(x) \in K[x]$ es un polinomio de grado n y $\alpha \in K$ es un elemento dado, podemos considerar la división

$$f(x) = (x - \alpha)f_1(x) + a_0,$$

donde observamos que, como $\mathrm{gr}(x - \alpha) = 1$, entonces $a_0 \in K$ y $\mathrm{gr}(f_1) = n - 1$.

Repitiendo lo anterior para $f_1(x)$ obtenemos

$$f_1(x) = (x-\alpha)f_2(x) + a_1,$$

con $a_1 \in K$ y $\operatorname{gr}(f_2) = n-2$.

Iterando este proceso obtenemos una sucesión de igualdades

$$\begin{aligned}
f(x) &= (x-\alpha)f_1(x) + a_0 \quad \text{con } \operatorname{gr}(f_1) = n-1\\
f_1(x) &= (x-\alpha)f_2(x) + a_1 \quad \text{con } \operatorname{gr}(f_2) = n-2\\
f_2(x) &= (x-\alpha)f_3(x) + a_2 \quad \text{con } \operatorname{gr}(f_3) = n-3\\
&\vdots\\
f_{n-1}(x) &= (x-\alpha)f_n(x) + a_{n-1} \quad \text{con } \operatorname{gr}(f_n) = n-n = 0,
\end{aligned}$$

y así $f_n(x)$ es constante, por lo que

$$f_n(x) = a_n \in K.$$

Substituyendo $f_1(x)$ en $f(x)$ y luego $f_2(x)$ en la igualdad resultante, etc., obtenemos

$$\begin{aligned}
f(x) &= a_0 + f_1(x)(x-\alpha)\\
&= a_0 + a_1(x-\alpha) + f_2(x)(x-\alpha)^2\\
&= a_0 + a_1(x-\alpha) + a_2(x-\alpha)^2 + f_3(x)(x-\alpha)^3\\
&\vdots\\
&= a_0 + a_1(x-\alpha) + a_2(x-\alpha)^2 + \cdots + a_n(x-\alpha)^n,
\end{aligned}$$

y así hemos probado:

TEOREMA VII.12. *Si $f(x) \in K[x]$ es un polinomio de grado n y $\alpha \in K$ es un elemento dado, entonces $f(x)$ se puede escribir de la forma*

$$f(x) = \sum_{k=0}^{n} a_k(x-\alpha)^k, \quad \text{con } a_k \in K. \qquad \square$$

EJERCICIO 14. Si $K = \mathbb{R}$, $f(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{R}$, recuerde la *expansión de Taylor* de la función real $f(x)$ y demuestre que los coeficientes a_k en (VII.12) son

$$a_k = \frac{f^{(k)}(\alpha)}{k!},$$

donde $f^{(k)}(x)$ es la k-ésima derivada de $f(x)$.

EJERCICIO 15. Exprese $f(x) = x^2 + 5x + 1$ en la forma $\sum a_k(x+1)^k$.

EJERCICIO 16. Exprese $f(x) = x^3 + x^2 + x + 1$ en la forma $\sum a_k(x-1)^k$.

VII.4 COEFICIENTES Y RAÍCES

Dado un polinomio $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, de grado $n \geq 1$ y con coeficientes en un campo K, dividiendo entre el coeficiente de grado $b_n \neq 0$, se obtiene un polinomio de la forma

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

en el cual el coeficiente de grado es $a_n = 1$. Un polinomio con coeficiente de grado 1 se dice que es *mónico*. Supongamos entonces que $\alpha_1, \ldots, \alpha_n$ son todas las raíces de $f(x)$, de tal forma que

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha_1) \cdots (x - \alpha_n).$$

Nuestro objetivo es obtener relaciones entre los coeficientes a_j de $f(x)$ y sus raíces α_k. Comencemos con el primer ejemplo no trivial, el caso cuando $f(x)$ es un polinomio cuadrático

$$f(x) = x^2 + a_1 x + a_0 = (x - \alpha_1)(x - \alpha_2).$$

Multiplicando los términos del lado derecho de esta igualdad, obtenemos

$$f(x) = x^2 + a_1 x + a_0 = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2,$$

de tal forma que

$$a_1 = -\alpha_1 - \alpha_2 \quad \text{y} \quad a_2 = (\alpha_1)(\alpha_2).$$

EJERCICIO 17. Para el polinomio cúbico $x^3 + a_2x^2 + a_1x + a_0$ obtenga las relaciones entre sus coeficientes y sus tres raíces $\alpha_1, \alpha_2, \alpha_3$.

Unos cuantos ejemplos más nos convencerán de que, si

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha_1) \cdots (x - \alpha_n),$$

entonces

$$\begin{aligned}
a_{n-1} &= -\alpha_1 - \cdots - \alpha_n && = \sum_{i=1}^{n}(-1)\alpha_i \\
a_{n-2} &= \sum_{1\le i<j\le n}(-\alpha_i)(-\alpha_j) && = \sum_{1\le i<j\le n}(-1)^2\alpha_i\alpha_j \\
a_{n-3} &= \sum_{1<i<j<k\le n}(-\alpha_i)(-\alpha_j)(-\alpha_k) && = \sum_{1\le i<j<k\le n}(-1)^3\alpha_i\alpha_j\alpha_k \\
&\vdots \\
a_0 &= (-\alpha_1)(-\alpha_2)\cdots(-\alpha_n) && = (-1)^n\alpha_1\alpha_2\cdots\alpha_n.
\end{aligned}$$

Es usual denotar a las sumas de productos de k factores ordenados de las raíces $\alpha_1, \ldots, \alpha_n$ como sigue

$$s_k(\alpha_1, \ldots, \alpha_n) := \sum_{1\le i_1<\cdots<i_k\le n} \alpha_{i_1}\cdots\alpha_{i_k}$$

y los s_k se conocen como los *polinomios simétricos elementales* de grado k en los $\alpha_1, \ldots, \alpha_n$. Así, las fórmulas anteriores se escriben

$$\begin{aligned}
a_{n-1} &= (-1)^1 s_1(\alpha_1, \ldots, \alpha_n) \\
a_{n-2} &= (-1)^2 s_2(\alpha_1, \ldots, \alpha_n) \\
a_{n-3} &= (-1)^3 s_3(\alpha_1, \ldots, \alpha_n) \\
&\vdots \\
a_0 &= (-1)^n s_n(\alpha_1, \ldots, \alpha_n)
\end{aligned}$$

y la validez de estas fórmulas es el contenido del teorema siguiente:

TEOREMA VII.13 (Fórmulas de Viète). *Sea $f(x) \in K[x]$ un polinomio mónico de grado n:*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

con raíces $\alpha_1, \ldots, \alpha_n$, repetidas de acuerdo con su multiplicidad. Entonces, los coeficientes a_i de $f(x)$ y sus raíces α_j se relacionan mediante las fórmulas

$$a_i = (-1)^{n-i}s_{n-i}(\alpha_1, \ldots, \alpha_n),$$

donde los $s_k(\alpha_1, \ldots, \alpha_n)$ son los polinomios simétricos elementales.

Demostración. Por inducción sobre n observando que los casos iniciales $n = 1$ y $n = 2$ son directos. Supongamos que el resultado es válido para polinomios de grado $< n$ y escribamos

$$f(x) = g(x)(x - \alpha_n) \quad \text{con } g(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$$

donde observamos que las raíces de $g(x)$ son $\alpha_1, \ldots, \alpha_{n-1}$ y satisfacen, por hipótesis de inducción, las fórmulas de Viète:

$$b_j = (-1)^{n-1-j} s_{n-1-j}(\alpha_1, \ldots, \alpha_{n-1}).$$

Ahora, de la igualdad $f(x) = g(x)(x - \alpha_n)$ se obtiene

$$\begin{aligned} x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 &= (x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0)(x - \alpha_n) \\ &= x^n + (b_{n-2} - \alpha_n)x^{n-1} + (b_{n-3} - \alpha_n b_{n-2})x^{n-2} \\ &\quad + \cdots + (b_0 - \alpha_n b_1)x - \alpha_n b_0, \end{aligned}$$

e igualando coeficientes obtenemos

$$\begin{aligned} a_{n-1} &= b_{n-2} - \alpha_n = (-1)^1 s_1(\alpha_1, \ldots, \alpha_{n-1}) - \alpha_n = -s_1(\alpha_1, \ldots, \alpha_n) \\ a_{n-2} &= b_{n-3} - \alpha_n b_{n-2} = (-1)^2 s_2(\alpha_1, \ldots, \alpha_{n-1}) - \alpha_n(-1)s_1(\alpha_1, \ldots, \alpha_{n-1}) \\ &= s_2(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_1(\alpha_1, \ldots, \alpha_{n-1}) \\ a_{n-3} &= b_{n-4} - \alpha_n b_{n-3} = (-1)^3 s_3(\alpha_1, \ldots, \alpha_{n-1}) - \alpha_n(-1)^2 s_2(\alpha_1, \ldots, \alpha_{n-1}) \\ &= (-1)^3[s_3(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_2(\alpha_1, \ldots, \alpha_{n-1})] \end{aligned}$$

y, en general,

$$(*) \qquad a_{n-k} = (-1)^k[s_k(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_{k-1}(\alpha_1, \ldots, \alpha_{n-1})]$$

donde observamos que

$$(\dagger) \qquad s_k(\alpha_1, \ldots, \alpha_n) = s_k(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_{k-1}(\alpha_1, \ldots, \alpha_{n-1})$$

para $1 \leq k \leq n - 1$ (simplemente separando, en la definición del polinomio $s_k(\alpha_1, \ldots, \alpha_n)$ los sumandos que no contienen a α_n y los que sí lo contienen). De esta observación y de $(*)$ se sigue que

$$a_{n-k} = (-1)^k s_k(\alpha_1, \ldots, \alpha_n),$$

que es lo que se quería probar, poniendo $i = n - k$. □

EJERCICIO 18. Demuestre formalmente la igualdad $(\dagger)$ anterior.

VII.5 Polinomios con coeficientes complejos

Consideremos ahora el caso especial de polinomios con coeficientes complejos, en particular con coeficientes reales. Dado un polinomio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{C}[x]$, se define $\overline{f}(x) := \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n \in \mathbb{C}[x]$. Observemos que $f(x) \in \mathbb{R}[x]$ si y sólo si $\overline{f}(x) = f(x)$.

Lema VII.14. (1) *Si* $f(x) = g(x)h(x)$ *en* $\mathbb{C}[x]$, *entonces* $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$.

(2) $f(x)|g(x)$ *en* $\mathbb{C}[x] \Leftrightarrow \overline{f}(x)|\overline{g}(x)$.

(3) *Si* $f(x) \in \mathbb{R}[x]$ *y* $\alpha \in \mathbb{C}$, *entonces*

$$(x-\alpha)^m|f(x) \Leftrightarrow (x-\overline{\alpha})^m|f(x).$$

(4) *Si* $f(x) \in \mathbb{R}[x]$ *y* $\alpha \in \mathbb{C}$ *es raíz de* $f(x)$, *entonces* $\overline{\alpha}$ *también es raíz de* $f(x)$ *y de la misma multiplicidad que* α. *Se sigue que el número de raíces imaginarias de* $f(x)$ *es par.*

Demostración. (1) Se sigue de la definición de producto de polinomios y de que el conjugado de una suma (producto) de complejos es la suma (producto) de los conjugados correspondientes. La parte (2) se sigue de (1). La parte (3) se sigue de (2) y del hecho que $\overline{f}(x) = f(x)$ porque $f(x)$ tiene coeficientes reales. La parte (4) se sigue de (3). □

Ejercicio 19. Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$ y suponga además que todos los $a_j \in \mathbb{Z}$. Si $\frac{a}{b} \in \mathbb{Q}$ es una raíz de $f(x)$ y además $\text{mcd}(a,b) = 1$, demuestre que $a|a_0$ y $b|a_n$.

Ejercicio 20. Si $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Q}[x]$ (note que el coeficiente a_n de x^n es precisamente $a_n = 1$) y suponga además que todos los $a_j \in \mathbb{Z}$. Demuestre que si $\alpha \in \mathbb{Q}$ es una raíz de $f(x)$ entonces $\alpha \in \mathbb{Z}$.

Ejercicio 21. Recuerde que, en general, dos polinomios $f(x), g(x) \in K[x]$ son iguales si y sólo si sus coeficientes correspondientes son iguales.

(1) Sean $f(x) = a_0 + a_1x + a_2x^2$ y $g(x) = b_0 + b_1x + b_2x^2$ dos polinomios cuadráticos en $\mathbb{C}[x]$. Suponga que para todo $\alpha \in \mathbb{C}$ se tiene que $f(\alpha) = g(\alpha)$. Demuestre que $f(x) = g(x)$.

(2) En general, si $f(x), g(x) \in \mathbb{C}[x]$ son tales que para todo $\alpha \in \mathbb{C}$ se tiene que $f(\alpha) = g(\alpha)$, demuestre que $f(x) = g(x)$.

(3) Lo anterior no es cierto en todos los campos. Encuentre dos polinomios $f(x), g(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ tales que $\forall \alpha \in \mathbb{Z}/2\mathbb{Z}$ se tiene que $f(\alpha) = g(\alpha)$ pero $f(x) \neq g(x)$.

El teorema fundamental del álgebra. Dado un polinomio $f(x) \in K[x]$ hemos visto que el número de raíces de $f(x)$ es $\leq \text{gr}(f)$ pero también notamos ahora que el número de raíces depende del campo donde se están considerando las raíces. Por ejemplo, el polinomio $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ no tiene raíces ni en $\mathbb{Q}$ ni en $\mathbb{R}$, y tiene dos raíces en $\mathbb{C}$, a saber, i y $-i$. El *teorema fundamental del álgebra* nos dice que un polinomio no cero $f(x) \in \mathbb{C}[x]$ de grado n tiene exactamente n raíces en $\mathbb{C}$ (contando multiplicidades, por supuesto) por lo que $f(x)$ se factoriza en polinomios lineales sobre $\mathbb{C}$:

$$f(x) = a(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r}$$

con los $\alpha_j \in \mathbb{C}$. Éste es el único teorema que usaremos sin demostrar en este libro. A pesar de su aparente simplicidad, su demostración involucra resultados que no hemos visto hasta ahora. Veamos unas aplicaciones de este teorema:

Ejemplo 2. En el anillo $\mathbb{C}[x]$ los únicos polinomios irreducibles son los de primer grado.

Demostración. En efecto, si $f(x) \in \mathbb{C}[x]$ tiene grado $n \geq 2$ entonces por el teorema fundamental del álgebra $f(x)$ tiene exactamente n raíces $\alpha \in \mathbb{C}$. Sea $\alpha \in \mathbb{C}$ una de estas raíces; por (VII.9) $(x - \alpha)|f(x)$ y por lo tanto $f(x)$ no es irreducible. □

Ejemplo 3. En el anillo $\mathbb{R}[x]$ los polinomios irreducibles tienen grado ≤ 2.

Demostración. Ya sabemos que los polinomios de primer grado son irreducibles. Ahora, como $\mathbb{R}[x] \subseteq \mathbb{C}[x]$, dado $f(x) \in \mathbb{R}[x]$ podemos pensarlo en $\mathbb{C}[x]$ y así, por el teorema fundamental del álgebra:

$$(*) \qquad f(x) = a(x - \alpha_1)^{m_1} \cdots (x - \alpha_t)^{m_t}$$

con $a, \alpha_j \in \mathbb{C}$. Observemos que a es el coeficiente de grado de $f(x) \in \mathbb{R}[x]$ por lo que $a \in \mathbb{R}$. Ahora, algunos de los α_j pueden ser reales y otros pueden ser complejos. Renumerando si hiciera falta podemos pensar que $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ y $\alpha_{r+1}, \ldots, \alpha_s \in \mathbb{C} - \mathbb{R}$. Sabemos, por (VII.14)(4) que las raíces complejas α de $f(x)$ satisfacen que sus conjugadas $\overline{\alpha}$ también son raíces de $f(x)$. Así, cada una de las raíces complejas $\alpha_{r+1}, \ldots, \alpha_s \in \mathbb{C} - \mathbb{R}$ de $f(x)$ aparece con su conjugada y por lo tanto debe haber un número par de ellas, es decir, $s - r = 2k$ y renumerando si hiciera falta podemos suponer que cada α_j está junta a su conjugada $\overline{\alpha}_j$, para $1 \leq j \leq k$. Entonces

$$\begin{aligned} f(x) &= a \cdot \prod_{j=1}^{r} (x - \alpha_j)^{m_j} \prod_{j-1}^{k} (x - \alpha_{r+j})^{m_{r+j}} (x - \overline{\alpha}_{r+j})^{m_{r+j}} \\ &= a \cdot \prod_{j=1}^{r} (x - \alpha_j)^{m_j} \prod_{j=1}^{k} \left((x - \alpha_{r+j})(x - \overline{\alpha}_{r+j})\right)^{m_{r+j}} \end{aligned}$$

y si ponemos $g_j(x) := (x - \alpha_{r+j})(x - \overline{\alpha}_{r+j}) = x^2 - (2\,\mathrm{Re}(\alpha_{r+j}))x + |\alpha_{r+j}|^2$, notamos que $2\,\mathrm{Re}(\alpha_{r+j})$ y $|\alpha_{r+j}|^2$ son reales por lo que $g_j(x) \in \mathbb{R}[x]$ y así

$$(\dagger) \qquad f(x) = a \cdot \prod_{j=1}^{r} (x - \alpha_j)^{m_j} \prod_{j=1}^{k} g_j(x)^{m_{r+j}}$$

con $(x - \alpha_j), g_j(x) \in \mathbb{R}[x]$. Más aún, como las dos raíces de cada $g_j(x)$ son complejas, entonces $g_j(x)$ es irreducible en $\mathbb{R}[x]$ y así $(\dagger)$ es la descomposición en factores irreducibles en $\mathbb{R}[x]$ de $f(x)$.

Se sigue que en $\mathbb{R}[x]$ sólo hay polinomios irreducibles de grado 1 (todos) y de grado 2 (algunos; de hecho aquellos polinomios cuadráticos que tengan discriminante $\Delta < 0$). □

Ejemplo 4. En el anillo $\mathbb{Q}[x]$ los polinomios $f(x) = x^2 - p$, con $p \in \mathbb{Z} \subseteq \mathbb{Q}$ primo, son irreducibles.

Demostración. En efecto, si $f(x)$ fuera compuesto se factorizaría en polinomios de primer grado, digamos

$$x^2 - p = (x - \alpha)(x - \beta)$$

con $\alpha, \beta \in \mathbb{Q}$. Se sigue que α, β son raíces cuadradas de p, las cuales no son racionales como vimos al principio del capítulo V, una contradicción. □

De hecho, se puede probar que para toda $n \geq 2$, si $p \in \mathbb{Z}$ es primo, entonces los polinomios $x^n - p$ son irreducibles en $\mathbb{Q}[x]$.

EJERCICIO 22. Demuestre que las dos afirmaciones siguientes son equivalentes:

1. Todo $f(x) \in \mathbb{C}[x]$ no constante tiene *todas* sus raíces en $\mathbb{C}$.
2. Todo $f(x) \in \mathbb{C}[x]$ no constante tiene *alguna* de sus raíces en $\mathbb{C}$.

EJERCICIO 23. Factorice en polinomios de primer grado en $\mathbb{C}[x]$ al polinomio $f(x) = x^5 - 1$.

EJERCICIO 24. El polinomio $f(x) = x^4 - 3x^3 - 6x^2 + 28x - 24$ tiene una raíz triple. Encuentre esta raíz y descomponga este polinomio en factores de primer grado en $\mathbb{C}[x]$.

EJERCICIO 25. El polinomio $f(x) = x^4 - 12x^3 + 48x^2 - 80x + 48$ tiene una raíz triple. Encuentre esta raíz y descomponga este polinomio en factores de primer grado en $\mathbb{C}[x]$.

EJERCICIO 26. El polinomio $f(x) = x^4 + 6x^3 + 13x^2 + 12x + 4$ tiene dos raíces dobles. Encuentre estas raíces y descomponga este polinomio en factores de primer grado en $\mathbb{C}[x]$.

EJERCICIO 27. Dado el polinomio $f(x) = x^5 - x \in \mathbb{R}[x]$, descompóngalo en factores irreducibles en $\mathbb{R}[x]$.

Haga lo mismo con el polinomio $g(x) = x^8 - 2 \in \mathbb{R}[x]$.

EJERCICIO 28. Muestre que el polinomio $f(x) = x^7 + x^3 + 1 \in \mathbb{C}[x]$, no tiene raíces múltiples.

VII.6 El campo de funciones racionales en una variable

Si K es un campo ya probamos que el anillo de polinomios $K[x]$ es un dominio entero y hemos visto que tiene propiedades análogas a las del anillo $\mathbb{Z}$. Recordemos ahora que partiendo de $\mathbb{Z}$ en el capítulo IV construimos el

campo $\mathbb{Q}$ de los números racionales mediante una relación de equivalencia en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. En $K[x]$ se tiene una construcción análoga: en el conjunto $K[x] \times (K[x] - \{0\})$ consideremos la relación siguiente:

$$(f(x), s(x)) \sim (g(x), t(x)) \quad \text{si} \quad f(x)t(x) = g(x)s(x).$$

De nuevo, la idea es pensar al par ordenado $(f(x), s(x))$ con $f(x) \in K[x]$ y $s(x) \in K[x] - \{0\}$ como a una *fracción* $\frac{f(x)}{s(x)}$. Se prueba fácilmente que $\sim$ es una *relación de equivalencia.* Al *conjunto cociente*

$$K[x] \times (K[x] - \{0\}) / \sim$$

se le denota $K(x)$ y a sus elementos, que son las clases de equivalencia de los pares $(f(x), s(x))$ con $s(x) \neq 0$, los denotamos mediante $\frac{f(x)}{s(x)}$ y se les llama *funciones racionales en una indeterminada* con coeficientes en K.

Se define una suma y un producto en $K(x)$ en forma similar a como se hizo en $\mathbb{Q}$:

Suma. Dados $\frac{f(x)}{s(x)}, \frac{g(x)}{t(x)}$ en $K(x)$ se eligen representantes $(f(x), s(x)) \in \frac{f(x)}{s(x)}$ y $(g(x), t(x)) \in \frac{g(x)}{t(x)}$ y se define:

$$\frac{f(x)}{s(x)} + \frac{g(x)}{t(x)} := \frac{f(x)t(x) + g(x)s(x)}{s(x)t(x)}.$$

Producto. Si $\frac{f(x)}{s(x)}, \frac{g(x)}{t(x)}$ en $K(x)$ se eligen representantes $(f(x), s(x)) \in \frac{f(x)}{s(x)}$ y $(g(x), t(x)) \in \frac{g(x)}{t(x)}$ y se define:

$$\frac{f(x)}{s(x)} \cdot \frac{g(x)}{t(x)} := \frac{f(x)g(x)}{s(x)t(x)}.$$

Ejercicio 29. Sea K un campo.

(1) Demuestre que la relación $\sim$ anterior es una relación de equivalencia en $K[x] \times (K[x] - \{0\})$.

(2) Demuestre que las operaciones anteriores están bien definidas en $K(x)$.

(3) Demuestre que con las operaciones anteriores, $K(x)$ es un campo, donde el cero es la clase de $(0, s(x))$ y el uno es la clase de $(s(x), s(x))$ para cualquier $s(x) \in K[x] - \{0\}$.

A $K(x)$ se le llama el *campo de funciones racionales en una variable con coeficientes en* K.

(4) Demuestre que la función natural $\phi : K \to K(x)$ que manda una constante $\alpha \in K$ en la fracción $\frac{\alpha}{1} \in K(x)$, es inyectiva y preserva las operaciones de K y $K(x)$.

Aun cuando los campos de funciones racionales $K(x)$, para cualquier campo K, son importantes, en esta parte final sólo consideraremos al campo $K = \mathbb{R}$ con el único objetivo de demostrar el *teorema de descomposición en fracciones parciales* en el campo $\mathbb{R}(x)$ que se usó en el curso de cálculo integral.

Recordemos lo que dice este teorema: dados polinomios $f(x), g(x) \in \mathbb{R}[x]$ con $g(x) \neq 0$, si $\text{gr}(f) \geq \text{gr}(g)$ podemos dividir $f(x)$ entre $g(x)$ y obtener

$$f(x) = g(x)q(x) + r(x) \quad \text{con } q(x), r(x) \in \mathbb{R}[x] \text{ y } \text{gr}(r) < \text{gr}(g).$$

Entonces, en el campo de funciones racionales $\mathbb{R}(x)$ se tiene que:

$$\frac{f(x)}{g(x)} = \frac{g(x)q(x) + r(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

con $\text{gr}(r) < \text{gr}(g)$. El resultado que buscamos nos dice que si $\text{gr}(r) < \text{gr}(g)$ entonces la fracción racional $\frac{r(x)}{g(x)}$ se descompone en suma de fracciones racionales *más simples*. Para explicar esto, descompongamos al polinomio $g(x)$ en factores irreducibles en $\mathbb{R}[x]$:

$$g(x) = a(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r}(x^2 + b_1x + c_1)^{n_1} \cdots (x^2 + b_sx + c_s)^{n_s}$$

con $a, \alpha_i, b_j, c_j \in \mathbb{R}$ y los factores primos diferentes en $\mathbb{R}[x]$, donde recordamos del ejemplo 3 anterior, que los polinomios primos de $\mathbb{R}[x]$ son de grado ≤ 1. La descomposición en fracciones parciales de $\frac{r(x)}{g(x)}$ está dada por:

TEOREMA VII.15. *Si $f(x), g(x) \in \mathbb{R}[x]$, con $g(x) \neq 0$ y si $g(x)$ se descompone en factores primos en $\mathbb{R}[x]$ como*

$$g(x) = a(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r}(x^2 + b_1x + c_1)^{n_1} \cdots (x^2 + b_sx + c_s)^{n_s}$$

con $a, \alpha_i, b_j, c_j \in \mathbb{R}$, entonces

$$\begin{aligned}\frac{f(x)}{g(x)} = q(x) &+ \frac{A_{1,1}}{(x-\alpha_1)^{m_1}} + \frac{A_{1,2}}{(x-\alpha_1)^{m_1-1}} + \cdots + \frac{A_{1,m_1-1}}{(x-\alpha_1)^2} + \frac{A_{1,m_1}}{(x-\alpha_1)} \\ &+ \frac{A_{2,1}}{(x-\alpha_2)^{m_2}} + \frac{A_{2,2}}{(x-\alpha_2)^{m_2-1}} + \cdots + \frac{A_{2,m_2-1}}{(x-\alpha_2)^2} + \frac{A_{2,m_2}}{(x-\alpha_2)} \\ &\vdots \\ &+ \frac{A_{r,1}}{(x-\alpha_r)^{m_r}} + \frac{A_{r,2}}{(x-\alpha_r)^{m_r-1}} + \cdots + \frac{A_{r,m_r-1}}{(x-\alpha_r)^2} + \frac{A_{r,m_r}}{(x-\alpha_r)} \\ &+ \frac{B_{1,1}x + C_{1,1}}{(x^2+b_1x+c_1)^{n_1}} + \frac{B_{1,2}x + C_{1,2}}{(x^2+b_1x+c_1)^{n_1-1}} + \cdots + \frac{B_{1,n_1}x + C_{1,n_1}}{(x^2+b_1x+c_1)} \\ &+ \frac{B_{2,1}x + C_{2,1}}{(x^2+b_2x+c_2)^{n_2}} + \frac{B_{2,2}x + C_{2,2}}{(x^2+b_2x+c_2)^{n_2-1}} + \cdots + \frac{B_{2,n_2}x + C_{2,n_2}}{(x^2+b_2x+c_2)} \\ &\vdots \\ &+ \frac{B_{s,1}x + C_{s,1}}{(x^2+b_sx+c_s)^{n_s}} + \frac{B_{s,2}x + C_{s,2}}{(x^2+b_sx+c_s)^{n_s-1}} + \cdots + \frac{B_{s,n_s}x + C_{s,n_s}}{(x^2+b_sx+c_s)},\end{aligned}$$

con $q(x) \in \mathbb{R}[x]$ *y los* $A_{i,j}, B_{i,j}, C_{i,j} \in \mathbb{R}$.

Demostración. La demostración será consecuencia de los dos lemas siguientes que, de alguna forma, capturan lo que es relevante en la masa de notaciones del teorema anterior.

El primer lema tiene en cuenta el hecho de que los factores en la descomposición de $g(x)$ son primos distintos y por lo tanto coprimos por pares:

LEMA VII.16. *Si* $g(x) = g_1(x)g_2(x)$ *en* $\mathbb{R}[x]$ *y* $\operatorname{mcd}(g_1, g_2) = 1$, *entonces para todo* $f(x) \in \mathbb{R}[x]$ *existen polinomios* $s_1(x), s_2(x) \in \mathbb{R}[x]$ *tales que*

$$\frac{f(x)}{g(x)} = \frac{s_1(x)}{g_1(x)} + \frac{s_2(x)}{g_2(x)}.$$

Demostración. Como $1 = \operatorname{mcd}(g_1, g_2)$, entonces existen $t_1(x), t_2(x) \in \mathbb{R}[x]$ tales que $1 = g_1t_1 + g_2t_2$ y así $f(x) = f(x)\cdot 1 = f(x)g_1(x)t_1(x) + f(x)g_2(x)t_2(x)$ por lo que:

$$\frac{f(x)}{g(x)} = \frac{f(x)g_1(x)t_1(x) + f(x)g_2(x)t_2(x)}{g_1(x)g_2(x)} = \frac{f(x)t_1(x)}{g_2(x)} + \frac{f(x)t_2(x)}{g_1(x)}$$

y se toman $s_1(x) := f(x)t_2(x)$ y $s_2(x) := f(x)t_1(x)$. □

El segundo lema tiene en cuenta cada factor primo de $g(x)$ junto con su exponente, digamos $h(x)^t$ con $t \geq 1$ y lo descompone en suma de fracciones:

LEMA VII.17. *Sean $f(x)$ y $h(x)$ en $\mathbb{R}[x]$ tales que $\operatorname{gr}(h) > 0$ y sea $t \geq 1$ un entero. Entonces existen polinomios $s_0(x), s_1(x), \ldots, s_t(x)$ en $\mathbb{R}[x]$ con $\operatorname{gr}(s_j) < \operatorname{gr}(h) =: n$ y tales que*

$$\frac{f(x)}{h(x)^t} = s_0(x) + \frac{s_1(x)}{h(x)^t} + \frac{s_2(x)}{h(x)^{t-1}} + \cdots + \frac{s_t(x)}{h(x)}.$$

Demostración. Consideremos las divisiones siguientes en $\mathbb{R}[x]$:

$$\begin{aligned} f &= hq_1 + r_1, \quad \operatorname{gr}(r_1) < \operatorname{gr}(h) = n \\ q_1 &= hq_2 + r_2, \quad \operatorname{gr}(r_2) < \operatorname{gr}(h) \\ q_2 &= hq_3 + r_3, \quad \operatorname{gr}(r_3) < \operatorname{gr}(h) \\ &\vdots \end{aligned}$$

y observemos que como $\operatorname{gr}(q_{i+1}) < \operatorname{gr}(q_i)$, entonces en algún momento $\operatorname{gr}(q_m) < n$ y así las divisiones anteriores terminan de la forma:

$$\begin{aligned} &\vdots \\ q_{m-1} &= hq_m + r_m, \quad \operatorname{gr}(r_m) < \operatorname{gr}(h) = n \\ q_m &= h \cdot 0 + q_m, \quad \operatorname{gr}(q_m) < \operatorname{gr}(h) = n. \end{aligned}$$

Substituyendo una ecuación en la otra queda:

$$\begin{aligned} f &= hq_1 + r_1 \\ &= h(hq_2 + r_2) + r_1 = h^2q_2 + hr_2 + r_1 \\ &= h^2(hq_3 + r_3) + hr_2 + r_1 \\ &= h^3q_3 + h^2r_3 + hr_2 + r_1 \\ &\vdots \\ &= h^mq_m + h^{m-1}r_m + h^{m-2}r_{m-1} + \cdots + hr_2 + r_1, \end{aligned}$$

por lo que

$$\frac{f}{h^t} = \frac{r_1}{h^t} + \frac{r_2}{h^{t-1}} + \cdots + \frac{r_t}{h} + \cdots$$

y se tienen dos casos: si $m \geq t$ al final queda un polinomio y si $m < t$ entonces quedan sólo fracciones de la forma deseada. □

El teorema de descomposición en fracciones parciales se sigue de estos dos lemas.

EJERCICIO 30. Provea los detalles de la demostración del teorema de descomposición en fracciones parciales.

EJERCICIO 31. Descomponga en fracciones parciales en $\mathbb{R}(x)$ las funciones racionales siguientes:

(1) $\dfrac{4x^2+13x-9}{x^3+2x^2-3x}$.

(2) $\dfrac{3x^3-18x^2+29x-4}{(x+1)(x-2)^2}$.

(3) $\dfrac{5x^3-3x^2+7x-3}{(x^2+1)^2}$.

VII.7 PROYECTO 4: POLINOMIOS TRUNCADOS Y CRIPTOSISTEMAS

Hasta ahora, hemos considerado polinomios con coeficientes en un campo K, pero también se tienen polinomios con coeficientes en un anillo arbitrario, y en este proyecto usaremos algunas propiedades de polinomios con coeficientes en $\mathbb{Z}$ o en $\mathbb{Z}/n\mathbb{Z}$. Si A es uno de estos anillos, denotaremos con $A[x]$ al conjunto de polinomios con coeficientes en A, es decir, los elementos de $A[x]$ son expresiones de la forma

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \quad \text{con } a_j \in A,$$

y decimos que dos polinomios son iguales si y sólo si tienen los mismos coeficientes.

EJERCICIO 32. Con la suma y producto de polinomios usuales, demuestre que si $A = \mathbb{Z}$ o $\mathbb{Z}/n\mathbb{Z}$, entonces $A[x]$ es un anillo conmutativo con uno. Muestre que $\mathbb{Z}[x]$ es un dominio entero (*sugerencia*: pruebe que el lema VII.2 vale en $\mathbb{Z}[x]$) pero que $(\mathbb{Z}/n\mathbb{Z})[x]$ no es dominio entero en general.

Divisibilidad. En el anillo $A[x]$ se tiene la noción usual de divisibilidad: si $f(x)$ y $g(x)$ son dos polinomios en $A[x]$ con $f(x) \neq 0$, diremos que $f(x)$ *divide* a $g(x)$ en $A[x]$, si existe otro polinomio $q(x) \in A[x]$ tal que $g(x) = f(x)q(x)$. Si $f(x)$ divide a $g(x)$ lo denotaremos por $f(x)|g(x)$.

EJERCICIO 33. Enuncie y demuestre las propiedades (III.14) en el anillo $A[x]$.

EJERCICIO 34. Demuestre que en $\mathbb{Z}[x]$ los únicos elementos que tienen inverso multiplicativo son los polinomios constantes ± 1.

EJERCICIO 35. Demuestre que en $(\mathbb{Z}/n\mathbb{Z})[x]$ los únicos elementos que tienen inverso multiplicativo son los polinomios constantes $u \neq 0$, con $u \in \mathbb{Z}/n\mathbb{Z}$ un elemento invertible en el anillo $\mathbb{Z}/n\mathbb{Z}$, *i.e.*, con u coprimo con n.

A los elementos de un anillo que tengan inverso multiplicativo se les llama *unidades* del anillo.

Anillos de polinomios truncados. Sea $N \geq 1$ un entero y sea A_N el conjunto de todos los polinomios de grado $\leq N-1$ con coeficientes en $\mathbb{Z}$. Así, los elementos de A_N son los polinomios

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1} \quad \text{con } a_j \in \mathbb{Z},$$

y como cada uno de estos polinomios está determinado por sus coeficientes, también lo podemos denotar mediante la N-ada ordenada:

$$f(x) \doteq [a_0, a_1, a_2, \ldots, a_{N-1}]$$

en $\mathbb{Z}^N = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (N factores). En esta notación la entrada a_j en el lugar j corresponde al monomio $a_j x^j$ (con la convención de que $x^0 = 1$). Por ejemplo, el polinomio $f(x) = 2 + 3x - x^3 + 5x^4 - 6x^7$, para $N = 8$ corresponde a la 8-ada ordenada $f(x) = [2, 3, 0, -1, 5, 0, 0, -6]$. Note, sin embargo, que es importante tener presente el parámetro N, ya que si $N = 10$ el mismo polinomio anterior corresponde a la 10-ada ordenada $f(x) = [2, 3, 0, -1, 5, 0, 0, -6, 0, 0]$. La notación de N-adas ordenadas es útil para almacenar polinomios en una computadora y calcular con ellos, como se verá más adelante.

Operaciones en A_N. En el conjunto A_N se tienen las operaciones suma y producto definidas como sigue:

SUMA. Los polinomios de A_N se suman en la forma usual, coeficiente a coeficiente.

PRODUCTO. Para definir un producto en A_N, recordemos que para el producto usual de polinomios se tiene que $x^i x^j = x^{i+j}$ y así al multiplicar dos polinomios en A_N (que tienen grado $\leq N-1$) algunos términos pueden tener grado $i+j \geq N$, y como queremos que el producto sea cerrado en A_N, eliminaremos estos términos x^k con $k \geq N$ mediante las reglas siguientes: la potencia x^N la reemplazamos por el entero 1, es decir, ponemos $x^N = 1$. Después, ponemos $x^{N+1} = x^N x = x$, es decir, reemplazamos x^{N+1} por x; similarmente x^{N+2} es reemplazado por x^2, etcétera. Entonces, el producto de polinomios de A_N, denotado $\star$, viene dado por el producto usual de polinomios, truncando las potencias de grado $\geq N$ de acuerdo con las reglas anteriores, de tal forma que el producto queda cerrado en A_N. Es fácil probar que, con las operaciones anteriores, el conjunto A_N resulta un anillo conmutativo con uno, al que llamaremos el *anillo de polinomios truncados* con coeficientes enteros.

Ejemplo 5. Si $N = 4$, consideremos los polinomios

$$f(x) = 3 + 2x + x^2 - 4x^3 \quad \text{y} \quad g(x) = 2 - x + 3x^2$$

en A_4, su suma es

$$f(x) + g(x) = (3+2) + (2-1)x + (1+3)x^2 + (-4+0)x^3 = 5 + x + 4x^2 - 4x^3$$

y su producto es

$$\begin{aligned} f(x) \star g(x) &= (3 + 2x + x^2 - 4x^3) \star (2 - x + 3x^2) \\ &= 6 - 3x + 9x^2 + 4x - 2x^2 + 6x^3 + 2x^2 - x^3 + 3x^4 - 8x^3 + 4x^4 - 12x \\ &= 6 + x + 9x^2 - 3x^3 + 4 - 12x \quad \text{ya que } x^4 = 1 \text{ y } x^5 = x \\ &= 10 - 11x + 9x^2 - 3x^3. \end{aligned}$$

Recordando la definición del producto usual, dados dos polinomios

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \quad g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

con $a_i, b_j \in \mathbb{Z}$, su producto

$$h(x) = f(x)g(x) = c_0 + c_1 x + \cdots + c_t x^t$$

es el polinomio cuyos coeficientes c_k están dados mediante la fórmula:

$$c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_ib_{k-i} + \cdots = \sum_{i+j=k} a_ib_j$$

entonces el producto $\star$ en el anillo A_N está dado por:

$$c_k = \sum_{i+j\equiv k \pmod N} a_ib_j.$$

EJERCICIO 36. Explique la fórmula anterior para c_k; en particular explique cómo la reducción módulo N equivale a las convenciones $x^N = 1$, $x^{N+1} = x$, etcétera.

EJERCICIO 37. Verifique que el conjunto A_N junto con las operaciones anteriores es, en efecto, un anillo conmutativo con uno.

Anillos de polinomios truncados módulo un entero. Como los coeficientes de un polinomio $f(x) = \sum a_ix^i$ en A_N son enteros, los podemos reducir módulo un entero $n \geq 1$ dado; es decir, dividimos cada coeficiente a_i de $f(x)$ entre n y tomamos su residuo. Usaremos la notación $f(x) \pmod n$ para indicar que los coeficientes de $f(x)$ se han reducido módulo n. El conjunto de polinomios truncados en N y reducidos módulo n forma un anillo conmutativo con uno, como el lector puede verificar fácilmente, y lo denotaremos mediante $A_{N,n}$.

EJERCICIO 38. Dados enteros $N \geq 2$ y $n \geq 1$, muestre que el conjunto $A_{N,n}$ de polinomios truncados en N y reducidos módulo n, con las operaciones suma y producto definidas usando la suma y producto de $\mathbb{Z}/n\mathbb{Z}$, es un anillo conmutativo con uno. Así, el anillo $A_{N,n}$ combina la aritmética modular (mód n) y la aritmética de polinomios truncados. Note que en el anillo $A_{N,n}$ la igualdad $f(x) = g(x) \pmod n$ quiere decir que los coeficientes de la diferencia $f(x) - g(x)$ son divisibles por n.

NOTA. En términos del álgebra abstracta, el anillo de polinomios truncados en N es el *anillo cociente* $A_N = \mathbb{Z}[x]/\langle x^N - 1\rangle$. Similarmente, el anillo $A_{N,n}$ es el anillo cociente $A_{N,n} = (\mathbb{Z}/n\mathbb{Z})[x]/\langle x^N - 1\rangle$.

Inversos multiplicativos en anillos de polinomios truncados. Al principio de esta sección, en el ejercicio 34, se le pedía al lector verificar que en $\mathbb{Z}[x]$

los únicos polinomios que tienen inverso multiplicativo son los polinomios constantes ± 1. Esto es análogo, y consecuencia, de que en $\mathbb{Z}$ los únicos elementos invertibles son precisamente ± 1. Sin embargo, en los anillos de polinomios truncados A_N y $A_{N,n}$ hay polinomios no constantes que son invertibles.

Ejemplo 6. Para $N = 6$ y $n = 2$, el polinomio

$$f(x) = 1 + x + x^2 + x^3 + x^5 \in A_{6,2} = (\mathbb{Z}/2\mathbb{Z})[x]/\langle x^6 - 1\rangle$$

tiene como inverso al polinomio

$$F_2(x) = 1 + x + x^3 + x^4 + x^5$$

ya que

$$\begin{aligned} f(x) \star F_2(x) &= (1 + x + x^2 + x^3 + x^5)(1 + x + x^3 + x^4 + x^5) \\ &= 1 + x + x^3 + x^4 + x^5 + x + x^2 + x^4 + x^5 + x^6 + x^2 + x^3 + x^5 \\ &\quad + x^6 + x^7 + x^3 + x^4 + x^6 + x^7 + x^8 + x^5 + x^6 + x^8 + x^9 + x^{10} \\ &= 1 + x + x^3 + x^4 + x^5 + x + x^2 + x^4 + x^5 + 1 + x^2 + x^3 + x^5 \\ &\quad + 1 + x + x^3 + x^4 + 1 + x + x^2 + x^5 + 1 + x^2 + x^3 + x^4 \\ &\quad \text{(truncando } x^6 = 1) \\ &= 5 + 4x + 4x^2 + 4x^3 + 4x^4 + 4x^5 \\ &= 1 \quad \text{(reduciendo módulo 2).} \end{aligned}$$

El algoritmo siguiente calcula el inverso del polinomio $a(x)$ en el anillo $A_{N,2} = (\mathbb{Z}/2\mathbb{Z})[x]/\langle x^N - 1\rangle$ con la condición de que $\text{mcd}(a(x), x^N - 1) = 1$. Note que en el paso 3 el número f_0 es el término independiente del polinomio $f(x)$:

Pseudocódigo para invertir un polinomio en $A_{N,2} = (\mathbb{Z}/2\mathbb{Z})[x]/\langle x^N - 1\rangle$:

`Entrada`: $a(x)$.

`Salida`: $b(x) = a(x)^{-1}$ `en` $A_{N,2} = (\mathbb{Z}/2\mathbb{Z})[x]/\langle x^N - 1\rangle$.

`Paso 1: Inicio`: $k := 0$, $b(x) := 1$, $c(x) := 0$, $f(x) := a(x)$, $g(x) := x^N - 1$.

Paso 2: Ciclo:

Paso 3: Mientras que $f_0 = 0$ hacer

Paso 4: $f(x) := f(x)/x$, $c(x) := c(x) \star x$, $k := k + 1$

Paso 5: Si $f(x) = 1$, entonces regresa $x^{N-k} b(x) \pmod{x^N - 1}$

Paso 6: Si $\mathrm{gr}(f) < \mathrm{gr}(g)$, entonces

Paso 7: intercambia f y g e intercambia b y c.

Paso 8: $f(x) := f(x) + g(x) \pmod 2$

Paso 9: $b(x) := b(x) + c(x) \pmod 2$

Paso 10: Fin del ciclo.

Usamos las rutinas anteriores para calcular el inverso del polinomio del ejemplo 6, $a(x) = 1 + x + x^2 + x^3 + x^5$ lo cual nos dio el resultado que llamamos $F_2(x)$ en el ejemplo 6.

Para la implementación del criptosistema NTRU también se requiere calcular el inverso de un polinomio no sólo módulo 2, sino también módulo una potencia de 2. Para hacer esto, primero se calcula el inverso del polinomio módulo 2 y luego se aplica una iteración como en el algoritmo siguiente para obtener el inverso del polinomio módulo 2^r:

Pseudocódigo para invertir un polinomio en $A_{N,2^r} = (\mathbb{Z}/2^r\mathbb{Z})[x]/\langle x^N - 1\rangle$:

Entrada: $a(x)$, r, $b(x) = a(x)^{-1} \pmod 2$.

Salida: $b(x) = a(x)^{-1}$ en $A_{N,2^r} = (\mathbb{Z}/2^r\mathbb{Z})[x]/\langle x^N - 1\rangle$.

Paso 1: $q = 2$.

Paso 2: Mientras que $q < 2^r$ hacer

Paso 3: $q = 2^2$

Paso 4: $b(x) := b(x)(2 - a(x)b(x)) \pmod q$

Note que en el paso 4 cambió el módulo de 2 a 2^2, etc., por lo que el producto $a(x)b(x)$ que es 1 módulo 2, ya no necesariamente es 1 módulo 2^2, etcétera.

Finalmente, para crear las claves pública y privada en el criptosistema NTRU también se requiere calcular inversos de polinomios módulo 3. El algoritmo siguiente calcula estos inversos:

Pseudocódigo para invertir un polinomio en $A_{N,3} = (\mathbb{Z}/3\mathbb{Z})[x]/\langle x^N - 1\rangle$:

Entrada: $a(x)$

Salida: $b(x) = a(x)^{-1}$ en $A_{N,3} = (\mathbb{Z}/3\mathbb{Z})[x]/\langle x^N - 1\rangle$.

Paso 1: Inicio: $k := 0$, $b(x) := 1$, $c(x) := 0$, $f(x) := a(x)$, $g(x) := x^N - 1$.

Paso 2: Ciclo:

Paso 3: Mientras que $f_0 = 0$ hacer

Paso 4: $f(x) := f(x)/x$, $c(x) := c(x) \star x$, $k := k + 1$

Paso 5: Si $f(x) = \pm 1$, entonces regresa $\pm x^{N-k} b(x)$ (mód $x^N - 1$)

Paso 6: Si $\mathrm{gr}(f) < \mathrm{gr}(g)$, entonces

Paso 7: intercambia f y g e intercambia b y c.

Paso 8: Si $f_0 = g_0$

Paso 9: $f(x) := f(x) - g(x)$ (mód 3)

Paso 10: $b(x) := b(x) - c(x)$ (mód 3)

Paso 11: De otra manera

Paso 12: $f(x) := f(x) + g(x)$ (mód 3)

Paso 13: $b(x) := b(x) + c(x)$ (mód 3)

Paso 14: Fin del ciclo.

NOTAS. En esta rutina los ± 1 en el paso 5 se eligen de tal forma que ambos tengan el mismo signo. Todos los cálculos se hacen módulo 3 escogiendo los representantes en el conjunto $\{-1, 0, 1\}$.

Observación. Sólo resta justificar por qué los algoritmos anteriores calculan, en efecto, el inverso del polinomio $a(x)$; esta justificación la daremos para el primer algoritmo, dejando los otros dos como un ejercicio para el lector interesado. Así, dado un polinomio $a(x) \in A_{N,2}$ coprimo con $m(x) = x^N - 1$,

la idea es considerar el vector (par ordenado) $(f, g) = (a, m)$ y multiplicarlo a la derecha por las matrices

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

para obtener, en cada uno de estos casos:

$$(f, g)A = (g, f), \qquad (f, g)B = (x^{-1}f, g), \qquad (f, g)C = (f + g, g)$$

notando entonces que el paso 7 del primer algoritmo es multiplicación por A, el paso 4 es multiplicación por B y el paso 8 es multiplicación por C. Observe además que en el paso 8 el polinomio $f + g$ tiene término constante cero y por lo tanto es divisible por x. En el paso 4 se divide a f por x hasta que el término constante sea constante $\neq 0$, *i.e.*, 1, y se regresa al paso 8 que garantiza que $f(x)$ tenga término constante cero. Note también que los pasos 6 y 7 aseguran que $\text{gr}(f) \geq \text{gr}(g)$. Finalmente, observe que cada paso por el ciclo reduce el grado total $\text{gr}(f) + \text{gr}(g)$ en al menos 1, en particular se reduce el grado de f y por lo tanto el algoritmo termina en a lo más $\text{gr}(f) + \text{gr}(g)$ iteraciones. Mostraremos ahora que el algoritmo produce al final el inverso de $a(x)$; para esto, observemos que al terminar las iteraciones se tiene un producto de matrices

$$(a, m)D_1 D_2 \cdots D_r = (\alpha, *) \tag{1}$$

donde cada matriz D_i es A, B o C y donde α es una constante $\neq 0$ módulo 2, es decir, $\alpha = 1$. Sin embargo, no sabemos que los coeficientes del producto

$$D_1 D_2 \cdots D_r \tag{2}$$

sean polinomios ya que la matriz B tiene a x^{-1} en una de sus entradas. Sea k el número de veces que B aparece en el producto (2). Entonces

$$x^k D_1 D_2 \cdots D_r$$

tiene coeficientes que son polinomios, digamos

$$x^k D_1 D_2 \cdots D_r = \begin{pmatrix} a' & * \\ m' & * \end{pmatrix}$$

y así multiplicando (1) por x^k obtenemos

$$x^k(\alpha, *) = (a, m)x^k D_1 \cdots D_r = (a, m)\begin{pmatrix} a' & * \\ m' & * \end{pmatrix} = (aa' + mm', *)$$

por lo que

$$aa' + mm' \equiv \alpha x^k \equiv x^k \text{ (mód } m), \quad \text{(ya que } \alpha = 1)$$

es decir,

$$aa' \equiv x^k \text{ (mód } m). \tag{3}$$

Para terminar observemos que el algoritmo que estamos analizando aplica las transformaciones $D_1 \cdots D_r$ al vector $(f, g) = (a, m)$ y al mismo tiempo se las aplica al vector $(b, c) = (1, 0)$ excepto que en el paso 4 en lugar de multiplicar por la matriz $B = \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ multiplica por la matriz $xB = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$. Ahora, como hemos supuesto que B se aplicó k veces, entonces al aplicar el algoritmo al vector inicial $(b, c) = (1, 0)$, el valor final del vector (b, c) es

$$(b, c) = (1, 0)x^k D_1 \cdots D_r = (1, 0)\begin{pmatrix} a' & * \\ m' & * \end{pmatrix} = (a', *),$$

es decir, el valor final del polinomio b es a' (mód m) y, por (3), satisface que

$$ab \equiv x^k \text{ (mód } m). \tag{4}$$

Ahora, como la constante $\alpha = 1$ es el valor final del polinomio f, *i.e*, $f = 1$, de (4) se sigue que

$$a^{-1} \equiv (x^k)^{-1} b \equiv x^{-k} b \equiv x^{N-k} b$$

(ya que $x^{-k} = x^{N-k}$ porque estamos trabajando módulo $m(x) = x^N - 1$). En otras palabras, el paso 5 regresa, en efecto, el inverso de $a(x)$.

El criptosistema de clave pública NTRU. En 1996, J. Hoffstein, J. Pipher y J. Silverman propusieron un nuevo método de encriptamiento de clave pública, basado en la aritmética del anillo de polinomios truncados en N módulo n, que es bastante rápido y seguro por lo que se ha posicionado como una alternativa seria al criptosistema RSA. En los párrafos siguientes describiremos brevemente una versión simplificada de este método.

Creación de la clave. Para implementar el sistema NTRU se requieren varios parámetros que, para simplificar, reduciremos a los siguientes: la persona, digamos Dan, que quiera crear uno de estos sistemas escoge:

- Un entero $N \geq 2$ para fijar el anillo A_N de polinomios truncados en N (esto explica las siglas del nombre del método NTRU: *tru*ncados en N).

- Un módulo q (grande) para fijar el anillo de polinomios truncados en N y reducidos módulo q.

- Un módulo pequeño p. Es esencial que los enteros p y q sean coprimos.

- Dos polinomios f, g en el anillo A_N elegidos aleatoriamente, es decir, tales que sus coeficientes se distribuyan aleatoriamente en el anillo $\mathbb{Z}/q\mathbb{Z}$. Además, se requiere que estos polinomios sean tales que sus coeficientes sean *pequeños* con respecto a q. Más precisamente, diremos que f es *pequeño* si tiene d_f coeficientes igual a $+1$ y $d_f - 1$ coeficientes igual a -1, y los demás igual a cero. Para el polinomio g se requiere que tenga d_g coeficientes igual a $+1$ y d_g coeficientes igual a -1, y los demás cero. Todo esto para enteros d_f y d_g elegidos previamente. La razón por la diferencia entre los $+1$ y -1 de f y g es que se quiere que f sea invertible en $A_{N,p}$ y $A_{N,q}$, mientras que para g no importa.

- Sean F_p y F_q los inversos multiplicativos de f módulo p y módulo q respectivamente, es decir,

$$F_p \star f = 1 \ (\text{mód } p) \quad \text{y} \quad F_q \star f = 1 \ (\text{mód } q).$$

- Después se calcula el producto

$$h = pF_q \star g \ (\text{mód } q).$$

La clave privada o secreta son los polinomios f y F_p (aunque también se sugiere mantener secreto el polinomio g).

La clave pública es el polinomio h y los enteros q, p y N.

Encriptar. Supongamos que Helen quiere enviar un mensaje a Dan usando las claves públicas (h, q, p, N) de Dan. Para comenzar, Helen convierte su texto en números, por ejemplo, usando las tablas que sirvieron para RSA. Después, Helen separa en bloques el número anterior cuidando que el número de bloques sea $\leq N$ y que cada bloque sea de tamaño $< p$. Estos bloques forman una N-ada $[b_0, b_1, b_2, \ldots, b_{N-1}]$ a la que Helen visualiza como un polinomio

$m(x)$ en $A_{N,p}$. Es aconsejable escoger los coeficientes b_j entre $-p/2$ y $p/2$ para que sean *pequeños* módulo q. Después, Helen escoge aleatoriamente un polinomio $\phi \in \mathbb{Z}[x]$ con coeficientes pequeños módulo q; este polinomio se usa para obscurecer más el proceso de encriptamiento. Finalmente, Helen utiliza la clave pública h de Dan para calcular

$$e = \phi \star h + m \text{ (mód } q)$$

y este polinomio $e = [e_0, e_1, \ldots, e_{N-1}]$ (mód q) es el mensaje encriptado que Helen envía a Dan.

Desencriptar. Para desencriptar el mensaje $e = e(x)$, Dan usa primero su clave privada f y calcula

$$a = f \star e \text{ (mód } q)$$

y escoge los coeficientes de $a(x)$ con representantes en el intervalo de $-q/2$ a $q/2$. Después, pensando al polinomio $a(x)$ con coeficientes enteros, reduce éstos módulo p para obtener $a(x)$ (mód p). Finalmente, Dan usa su otra clave privada F_p y calcula el producto

$$b = F_p \star a \text{ (mód } p).$$

Observamos ahora que $b(x) = m(x)$ es el mensaje original, ya que

$$\begin{aligned}
a &= f \star e \text{ (mód } q) \quad \text{por definición de } a(x) \\
&= f \star (\phi \star h + m) \text{ (mód } q) \quad \text{por definición de } e(x) \\
&= f \star \phi \star h + f \star m \text{ (mód } q) \\
&= f \star \phi \star pF_q \star g + f \star m \text{ (mód } q) \quad \text{por definición de } h(x) \\
&= p\phi \star (f \star F_p) \star g + f \star m \text{ (mód } q) \\
&= p\phi \star g + f \star m \text{ (mód } q) \quad \text{ya que } f \star F_q = 1 \text{ (mód } q).
\end{aligned}$$

Ahora, consideremos este último polinomio $p\phi \star g + f \star m$ y observemos que todos sus ingredientes tienen coeficientes pequeños con respecto a q, y como p también es pequeño con respecto a q, entonces los coeficientes de este polinomio están entre $-q/2$ y $q/2$, de tal forma que al reducirlo módulo q no cambian. Es decir, Dan ha recuperado el polinomio

$$a = p\phi \star g + f \star m \quad \text{en } A = \mathbb{Z}[x]/\langle x^N - 1 \rangle.$$

Finalmente, Dan reduce este último polinomio módulo p y obtiene

$$a = f \star m \ (\text{mód } p) \quad \text{ya que } p\phi \star g = 0 \ (\text{mód } p),$$

y luego multiplica por F_p para recuperar $m(x)$:

$$\begin{aligned} F_p \star a &= F_p \star f \star m \ (\text{mód } p) \\ &= m \ (\text{mód } p) \quad \text{ya que } F_p \star f = 1 \ (\text{mód } p). \end{aligned}$$

EJERCICIO 39. El ejercicio mayor de este proyecto es implementar los pseudocódigos de NTRU.

EJERCICIO 40. Use los parámetros pequeños siguientes para ilustrar el método: $N = 16$, $q = 2^5 = 32$, $p = 3$, $d_f = 6$, $d_g = 5$.

- Cree claves públicas y privadas eligiendo polinomios de grado ≤ 15.
- Encripte las palabras HOLA y CASA.
- Desencripte los mensajes anteriores comprobando que recupera las palabras del inciso anterior.

La notación ternaria balanceada. Estamos acostumbrados a escribir números y hacer aritmética en el sistema decimal (base 10) y el sistema binario (base 2); en el sistema decimal los dígitos que usamos son: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, y en el sistema binario los dígitos son: 0, 1. Para su uso en el sistema de encriptamiento NTRU, introduciremos aquí la *notación ternaria balanceada* para representar un número (real). Como su nombre lo indica, éste es un sistema con base 3, es decir, los números se representan como sumas de potencias con exponente entero, de la base 3, pero en lugar de usar los dígitos 0, 1, 2, se usan los dígitos -1, 0, 1. En este sentido el sistema de numeración es *balanceado* porque sus dígitos están repartidos simétricamente con respecto del cero. Para facilidad de la notación se suele representar al dígito -1 como $\bar{1}$ con el signo menos arriba del uno. Por ejemplo, el numeral ternario $10\bar{1}1$ representa al número

$$10\bar{1}1 = 1 \times 3^3 + 0 \times 3^2 - 1 \times 3^1 + 1 \times 3^0 = 27 + 0 - 3 + 1 = 25.$$

Los naturales del 1 al 10, en notación ternaria balanceada son:

$$1, 11, 10, 11, 1\bar{1}\bar{1}, 110, 1\bar{1}1, 101, 100, 101.$$

Para mayor información acerca de la notación ternaria balanceada, véase, por ejemplo, la referencia [2].

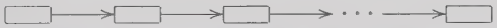
VII.7.1 Bibliografía

[1] Hofffstein, J., J. Pipher, J. Silverman, "NTRU: A ring-based public key criptosystem", en Joe P. Buhler (comp.), *Algorithmic Number Theory* (ANTS III), Lecture Notes on Computer Science 1423, Springer-Verlag, Berlín, 1998, pp. 267-288.

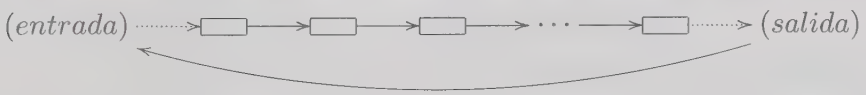
[2] Knuth. D. E., *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 2ª ed., Addison-Wesley, Reading, Mass., pp. 190-193.

VII.8 Proyecto 5: Registros de corrimiento

Usando polinomios y, al final, un poco de álgebra lineal, en este proyecto estudiaremos los aspectos iniciales de los registros de corrimiento (o desplazamiento). Podemos pensar a un *registro de corrimiento* como un dispositivo formado por un cierto número de casillas, digamos n, colocadas una junto a la otra en línea recta:



donde en cada casilla o registro se tiene asignado un dígito y se tiene un mecanismo que hace que el registro nos provea de un dígito a cada tic de un reloj mediante un corrimiento de los dígitos de una casilla a la casilla adyacente a la derecha, de tal manera que el dígito de salida se mueve ahora a la casilla de entrada, recorriendo un lugar todos los otros dígitos:



La casilla o registro del extremo izquierdo se llama el *registro de alimentación* y la casilla del extremo derecho se llama el *registro de salida.*

Una vez que el registro de corrimiento comienza a funcionar, seguirá produciendo dígitos de salida indefinidamente, sin necesidad de control o alimentación externos.

Los registros más sencillos proveen el dígito de salida como una combinación lineal fija de los dígitos almacenados en los n registros del dispositivo. Así, si numeramos los registros de izquierda a derecha comenzando con el 0 y terminando con el $n-1$ de tal forma que los registros son R_0, R_1, R_2,..., R_{n-1} y si los parámetros que dan la combinación lineal fija son $a_0, a_1, a_2, \ldots, a_{n-1}$, entonces la combinación lineal de los registros R_i es:

$$a_0R_0 + a_1R_1 + a_2R_2 + \cdots + a_{n-1}R_{n-1}.$$

Ahora, si los registros contienen los dígitos iniciales $g_0, g_1, g_2, \ldots, g_{n-1}$:

$$\boxed{g_0} \longrightarrow \boxed{g_1} \longrightarrow \boxed{g_2} \longrightarrow \cdots \longrightarrow \boxed{g_{n-1}}$$

se tiene que el primer dígito de salida es

$$g_n = a_0g_0 + a_1g_1 + a_2g_2 + \cdots + a_{n-1}g_{n-1}$$

el cual se coloca en el registro de alimentación recorriendo los dígitos restantes:

$$\boxed{g_n} \longrightarrow \boxed{g_0} \longrightarrow \boxed{g_1} \longrightarrow \cdots \longrightarrow \boxed{g_{n-2}}$$

y el dígito de salida siguiente es:

$$g_{n+1} = a_0g_n + a_1g_0 + a_2g_1 + \cdots + a_{n-1}g_{n-2};$$

en general, si $k \geq n$, el dígito g_k está dado por la fórmula de recurrencia:

$$g_k = a_{n-1}g_{k-1} + a_{n-2}g_{n-2} + \cdots + a_0g_{k-n}.$$

Observemos ahora que del registro de corrimiento sólo nos interesan los lugares o casillas R_k y estos lugares los podemos indicar por el monomio X^k, de tal forma que R_0 corresponde a X^0, R_1 corresponde a X^1,..., R_{n-1} corresponde a X^{n-1}. Entonces, la combinación lineal $a_0R_0 + a_1R_1 + a_2R_2 + \cdots + a_{n-1}R_{n-1}$ de los registros corresponde a la expresión

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_{n-1}X^{n-1}$$

y podemos pensar a

$$f = a_0 + a_1X^1 + a_2X^2 + \cdots + a_{n-1}X^{n-1}$$

como a un polinomio en la variable X, con coeficientes a_k.

El problema inicial es ver cómo este polinomio se relaciona con el registro de corrimiento que en forma recurrente nos da la salida

$$g_k = a_{n-1}g_{k-1} + a_{n-2}g_{n-2} + \cdots + a_0 g_{k-n} \quad \text{para } k \geq n.$$

Con este objetivo, consideremos en lugar de f al polinomio

$$s = a_{n-1}X + a_{n-2}X^2 + \cdots + a_1 X^{n-1} + a_0 X^n$$

y también al polinomio

$$t = \sum_{j=0}^{n-1} \left(g_j - \sum_{i=1}^{j} a_{n-i} g_{j-i} \right) X^j,$$

donde $g_0, g_1, \ldots, g_{n-1}$ son los dígitos iniciales del registro de corrimiento.

TEOREMA VII.18. *En un registro de corrimiento con polinomio* $f = a_0 + a_1X^1 + a_2X^2 + \cdots + a_{n-1}X^{n-1}$ *y dígitos iniciales* $g_0, g_1, \ldots, g_{n-1}$ *(en un anillo conmutativo con uno), el dígito de salida* g_k*, para* $k \geq n$*, es el coeficiente de* X^k *en el producto*

$$(1 + s + s^2 + \cdots + s^k)t$$

para s *y* t *como antes.*

Demostración. Observemos primero que, como los dígitos g_i se van generando recursivamente, en general $g := \sum_i g_i X^i$ no es un polinomio ya que puede haber un número infinito de $g_i \neq 0$; sin embargo, si fijamos un natural k podemos pensar en la parte de g de grado $\leq k$, es decir, desechamos los términos de grado $> k$ para obtener el polinomio $\sum_{i=1}^{k} g_i X^i$. Al desechar los términos de grado $> k$ usaremos la frase: *salvo múltiplos de* X^{k+1}. Con esto, lo que deseamos probar es que el coeficiente g_k de X^k en g es el coeficiente de X^k en el producto $(1 + s + s^2 + \cdots + s^k)t$; es decir, queremos probar que se tiene la igualdad (salvo múltiplos de X^{k+1}):

$$g = (1 + s + s^2 + \cdots + s^k)t.$$

Para probar esto, observemos que, salvo múltiplos de X^{k+1},

$$\begin{aligned} sg &= (a_{n-1}X + a_{n-2}X^2 + \cdots + a_0 X^n)(g_0 + g_1 X + \cdots + g_k X^k) \\ &= \sum_{j=0}^{k} \sum_{i=1}^{n} a_{n-i} g_{j-i} X^j \end{aligned}$$

y así, poniendo $g_r = 0$ para $r < 0$, salvo múltiplos de X^{k+1}, tenemos que

$$\begin{aligned} g - sg &= (g_0 + g_1 X + \cdots + g_k X^k) - \sum_{j=0}^{k} \sum_{i=1}^{n} a_{n-i} g_{j-i} X^j \\ &= \sum_{j=0}^{k} \left(g_j - \sum_{i=1}^{n} a_{n-i} g_{j-i} \right) X^j \\ &= \sum_{j=0}^{n-1} \left(g_j - \sum_{i=1}^{j} a_{n-i} g_{j-i} \right) X^j \quad \text{(por la fórmula de recurrencia)}, \end{aligned}$$

es decir, salvo múltiplos de X^{k+1},

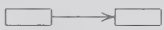
$$(1 - s)g = t.$$

Se sigue que, salvo múltiplos de X^{k+1},

$$(1 + s + s^2 + \cdots + s^k)t = (1 + s + s^2 + \cdots + s^k)(1 - s)g = (1 - s^{k+1})g = g$$

(la última igualdad es porque s^{k+1} sólo contiene múltiplos de X^{k+1}, *i.e.*, $s^{k+1} = 0$ salvo múltiplos de X^{k+1}). □

Ejemplo 9. Consideremos un registro con dos casillas:



con polinomio de corrimiento $f = 1 + X \in \mathbb{Z}[X]$ y dígitos iniciales $g_0 = 1 = g_1$. El k-ésimo registro (para $k \geq 2$) está dado por la fórmula de recurrencia

$$g_k = g_{k-2} + g_{k-1}$$

y observamos que la sucesión de dígitos de salida es la sucesión de Fibonacci. Ahora, los polinomios s y t del teorema anterior están dados por

$$t = (g_0 - 0) + (g_1 - a_1 g_0)X = g_0 + (g_1 - g_0)X = 1$$

y

$$s = a_1 X + a_0 X^2 = X + X^2,$$

y por lo tanto el dígito g_k es el coeficiente de X^k en el producto

$$(1 + s + s^2 + \cdots)t = 1 + (X + X^2) + (X + X^2)^2 + (X + X^2)^3 + \cdots.$$

EJERCICIO 41. Compare el resultado anterior con el ejemplo 18 en § II.7.1.

Para un registro de corrimiento con polinomio $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ el punto importante es cómo pasar del estado k al estado $k+1$ y esto se puede expresar en el lenguaje de matrices del álgebra lineal como sigue: al polinomio f se le asocia la matriz $n \times n$:

$$R = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}$$

con entradas en el anillo A donde se encuentran los coeficientes a_i del polinomio f. Se pide al lector investigar o recordar cómo se opera con matrices (suma y producto de matrices). Una vez hecho esto, debe ser fácil probar que:

EJERCICIO 42. La transición del estado k del registro al estado $k+1$ está dada por

$$(g_{k-n+1}, \ldots, g_k) = (g_{k-n}, \ldots, g_{k-1}) \cdot R$$

donde en la derecha se tiene el producto de una matriz $1 \times n$ por una matriz $n \times n$.

BIBLIOGRAFÍA

Algunas observaciones y comentarios sobre la bibliografía: el libro [2] contiene muchos de los temas tratados en nuestro texto, pero difiere en el enfoque general y en temas particulares, como en el estudio de los números naturales, algunos temas de nuestro capítulo III, sobre el orden en los racionales, y todo sobre el campo de los números reales. Del libro [8], sólo sugerimos, en este momento, la lectura del primer capítulo, donde se estudia el campo $\mathbb{R}$. El libro de Landau [10] es un clásico y, como algunos buenos vinos, es frío, seco, distante; su lectura siempre es estimulante y contiene parte de los temas tratados en el capítulo II, las primeras dos secciones del capítulo III, parte del capítulo IV, y un enfoque diferente para la construcción de los números reales, usando *cortaduras de Dedekind*, lo cual también puede verse en el capítulo inicial del libro de Rudin [14]. Si la lectora o lector sienten curiosidad por la lógica matemática, [15] es un buen lugar para comenzar.

[1] Adleman, L., R. L. Rivest, A. Shamir, "A method for obtaining digital signatures and public-key cryptosystems", *Comm. ACM* **21** (1978), 120-126.

[2] Cárdenas, H., E. Lluis, F. Raggi, F. Tomás, *Álgebra superior,* Trillas, México, 1999.

[3] Coutinho, S. C., *The Mathematics of ciphers,* A. K. Peters, Wellesley (Massachusetts), 1999.

[4] Diffie, W., M. E. Hellman, "New directions in cryptography", *IEEE Trans. on Information Theory,* **22**, 1976, 644-654.

[5] Euclides, *Elementos: Libros V-IX,* Gredos, Madrid, 1994.

[6] Gouvêa, F., *p-adic numbers.* Springer Verlag, Berlín, 1993.

[7] Halmos, P., *Naive Set Theory.* Springer Verlag, Berlín, 1993.

[8] Hewitt, E., K. Stromberg, *Real and Abstract Analysis,* Springer Verlag, Berlín, 1965.

[9] Hofffstein, J., J. Pipher, J. Silverman, "NTRU: A ring-based public key criptosystem", en Joe P. Buhler (comp.), *Algorithmic Number Theory*

(ANTS III), Lecture Notes on Computer Science 1423, Springer-Verlag, Berlín, 1998, 267-288.

[10] Landau, E., *Foundations of Analysis*, 3ª ed., Chelsea, Nueva York, 1966.

[11] Lang, S., *Linear Algebra*, Springer Verlag, Nueva York, 2000.

[12] Pineda, M., *Aritmética y teoría de grupos*, UAM, México, 1995.

[13] Rincón, H., *Cuando cuentes cuántos*, Temas de Matemáticas para Bachillerato, Instituto de Matemáticas, UNAM, México, 2002.

[14] Rudin, W., *Principles of Mathematical Analysis*, McGraw-Hill, Nueva York, 1964.

[15] Solís, J., Y. Torres, *Lógica matemática*, UAM, México, 1995.

[16] Verde-Star, L., *Matemática discreta y combinatoria*, Anthropos, Barcelona, 1996.

[17] Weil, A., *Number Theory: An approach through history from Hammurapi to Legendre*. Birkhäuser Verlag, Boston, Massachusetts, 2001.

[18] Zaldívar, F., "El pequeño teorema de Fermat", *Misc. Mat.*, **34**, 2001, 73-84.

ÍNDICE DE TÉRMINOS

algoritmo
  de la división entre polinomios, 270
  de Euclides
    entre polinomios, 274
  de Euclides en $\mathbb{Z}$, 149
  de la división en $\mathbb{Z}$, 144
anillo, 132
  $\mathbb{Z}/m\mathbb{Z}$, 165
  de polinomios, 267
    truncados, 297
  con uno, 132
  conmutativo, 132
  de enteros $\mathbb{Z}$, 130
  de enteros módulo m, 164
árbol, 119
  arraigado, 119
  binario, 119
argumento de un complejo, 257
aristas, 119
aritmética modular, 165
asociatividad
  de la suma en $\mathbb{N}$, 58
  del producto en $\mathbb{N}$, 61
axioma, 51
  de elección, 48
  de inducción, 51
axiomas de Peano, 51

buen orden, 72

campo, 167, 232
  completo, 219
  de funciones racionales, 291
  de los números reales, 215
  de números complejos, 249
  arquimediano, 244
  completo, 244
  de los números p-ádicos, 230
  de los números racionales, 199
cardinal, 74
cero de un polinomio, 276
ciclo, 119
clase de equivalencia, 34
clase positiva
  en $\mathbb{R}$, 217
  en $\mathbb{Q}$, 201
  en $\mathbb{Z}$, 137
clases residuales, 164
codominio, 39
coeficiente de grado, 268
coeficientes binomiales, 97
combinaciones, 93
complemento, 24
completez de $\mathbb{R}$, 221
composición, 43
compuesto, 152
conectivos lógicos, 16
congruencias, 162
congruencias lineales, 168
conjugación, 253
conjunción, 14
conjunto, 20
  cociente, 35
  finito, 74
  infinito, 74
  parcialmente ordenado, 37
  totalmente ordenado, 71
  vacío, 22

conmutatividad
de la suma en $\mathbb{N}$, 58
del producto en $\mathbb{N}$, 60
coprimos, 147
cortaduras de Dedekind, 226
cota
inferior, 222, 241
superior, 222, 241
criba de Eratóstenes, 153
criptografía, 181
criptosistema RSA, 182
cuantificador
existencial, 19
universal, 18

definición recursiva, 56
derivada de un polinomio, 281
desarreglo, 103
desarrollo binomial, 98
con exponentes negativos, 116
diferencia, 24
Diofanto, 158
distributividad
en $\mathbb{N}$, 61
disyunción, 15
divisibilidad, 145
divisor, 145
divisor de cero, 140
dominio
de una función, 39
de una relación, 30
dominio entero, 140

ecuaciones diofantinas, 158
elementos, 20
enumerar, 77
equivalencia, 15
Euclides, 148
existencia de $\mathbb{N}$, 52
expansión de Taylor, 283

factor, 145
factorial, 92
familia de conjuntos, 27
forma $a + bi$, 252
forma polar de un complejo, 258
fórmula cerrada, 68, 108
fórmula recursiva, 68, 108
fórmulas de De Moivre, 260
función, 38
biyectiva, 40
característica, 50, 82
de Euler, 177
exponencial, 117
generadora, 116, 117
identidad, 39
inyectiva, 40
logaritmo, 117
sucesor, 51
suprayectiva, 40

grado de un polinomio, 268
gráfica
conexa, 119
de una función, 39
plana, 119

hipótesis de inducción, 53

igualdad, 22
igualdad de funciones, 40
imagen, 39
de un conjunto, 49
inversa de un conjunto, 49
implicación, 15
ínfimo, 223, 242
infinitud del conjunto de primos, 157
intersección, 23
intervalo de naturales, 74

inversa
bilateral, 46
de una función, 44
derecha, 46
izquierda, 46
inverso multiplicativo, 138

leyes
de De Morgan, 25
distributivas, 25
límite, 209
lista, 77

máximo común divisor, 146
máximo común divisor de polinomios, 273
mínimo común múltiplo, 156
módulo de un complejo, 253
multiplicidad, 278
múltiplo, 145

negación, 14
notación ternaria balanceada, 306
número de Carmichael, 180
números
p-ádicos, 230
complejos, 247
enteros, 127
naturales, 51
racionales, 197
reales, 215

orden
en $\mathbb{R}$, 217
en $\mathbb{N}$, 62
en $\mathbb{Q}$, 201
en $\mathbb{Z}$, 136
parcial, 37, 70
total, 70
ordenaciones, 91
con repetición, 89

parte imaginaria de un complejo, 252
parte real de un complejo, 252
partición, 35
paso inductivo, 53
permutación, 92
polinomio, 267
constante, 267
primo o irreducible, 274
polinomios simétricos elementales, 285
postulado, 51
precede, 62
primer elemento, 72
primer teorema de Euclides, 151
primo, 152
primos relativos, 147
principio
básico de la suma, 78
básico del producto, 80
de inclusión-exclusión, 103
de inducción, 64
de la suma, 79
del buen orden, 72
del palomar, 77, 79
del producto, 81
generalizado del producto, 87
principios elementales de conteo, 77
producto
de polinomios, 267
en $\mathbb{C}$, 248
en $\mathbb{N}$, 59
en $\mathbb{Q}$, 198
en $\mathbb{R}$, 215
en $\mathbb{Z}$, 128
en $\mathbb{Z}/m\mathbb{Z}$, 164
producto cartesiano, 30
propiedad arquimediana
de $\mathbb{Q}$, 204
de $\mathbb{R}$, 220
proposición, 14

raíces de complejos, 260
raíz
múltiple, 278
simple, 278
de un polinomio, 276
registro
de alimentación, 307
de corrimiento, 307
de salida, 307
regla de correspondencia, 38
reglas de los signos, 133
relación, 30
de inclusión, 21
de pertenencia, 20
antisimétrica, 31
de equivalencia, 32
reflexiva, 31
simétrica, 31
total, 31
transitiva, 31
vacía, 31

sistema de Peano, 54
subconjunto, 21
subsucesión, 210
sucesión, 208
acotada, 211
de Cauchy, 211
binaria, 106
convergente, 209
de Fibonacci, 69, 109
tipo Fibonacci, 110
sucesor, 51
suma
de polinomios, 267
en $\mathbb{R}$, 215
en $\mathbb{Z}$, 128
en $\mathbb{C}$, 248
en $\mathbb{N}$, 57
en $\mathbb{Q}$, 198
en $\mathbb{Z}/m\mathbb{Z}$, 164
supremo, 223, 241

tabla, 83
tabla de verdad, 14
teorema
de descomposición en fracciones parciales, 292
del residuo, 277
fundamental del álgebra, 288
chino del residuo, 172
de Euler, 179
fundamental de la aritmética, 154
pequeño de Fermat, 176
torres de Hanoi, 67
triángulo de Pascal, 96
tricotomía, 71
en $\mathbb{N}$, 63
en $\mathbb{Q}$, 202
en $\mathbb{R}$, 218
en $\mathbb{Z}$, 136

unicidad de $\mathbb{N}$, 55
unidad, 296
unidad imaginaria, 252
unión, 23

valor absoluto
p-ádico, 228
en $\mathbb{R}$, 219
en $\mathbb{Q}$, 204
en $\mathbb{Z}$, 138
no arquimediano, 229
valor de verdad
falso, 14
verdadero, 14
vértices, 119

Fundamentos de álgebra
se terminó de imprimir y encuadernar
en octubre de 2005 en los talleres
de Impresora y Encuadernadora Progreso, S.A. de C.V. (IEPSA),
calzada de San Lorenzo 244, 09830 México, D.F.

Se tiraron 1 000 ejemplares

Tipografía y formación en LaTeX 2_ε,
con tipos Computer Modern de 11:14 pts.

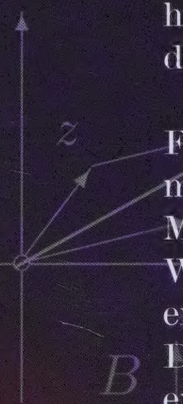
Corrección: *Kenia Salgado, Ricardo Rubio*
y *el autor*

Cuidó la edición *Axel Retif*

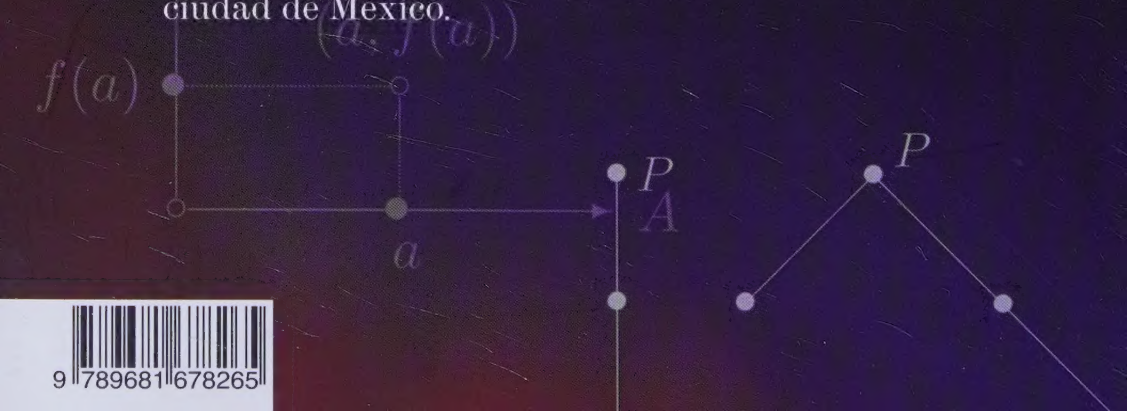
Coordinación editorial:
María del Carmen Farías

En este libro —nos dice el autor en su Prólogo— se parte de unas ideas sencillas de lógica y conjuntos que formalizan, hasta donde es posible en un nivel elemental, el lenguaje que se usará a todo lo largo y ancho del texto, incluyendo la notación e ideas básicas de la teoría de conjuntos, que permean la matemática. Una vez desarrollado lo anterior, el libro comienza propiamente: relaciones y funciones son conceptos fundamentales en toda la matemática y se discuten con la amplitud necesaria. Después, usando el lenguaje e ideas anteriores, empieza el estudio de las estructuras numéricas: números naturales, enteros, racionales, reales y complejos. El método es simple: se comienza elementalmente y se avanza construyendo sobre lo discutido previamente.

A lo largo del texto se incluyen ejercicios que complementan lo estudiado previamente. Los ejercicios son importantes, y se requiere que los lectores los vayan haciendo conforme avanza el libro: la matemática es un deporte de participantes y no de espectadores.



Felipe Zaldívar estudió la licenciatura y maestría en matemáticas en la Universidad Nacional Autónoma de México, y obtuvo el doctorado en la University of Western Ontario, en Canadá. Ha sido profesor visitante en la George Washington University, en Washington, D.C., y actualmente es profesor titular de matemáticas en la Universidad Autónoma Metropolitana-I, en la ciudad de México.



9 789681 678265